KATHO
KATHOLIEKE HOGESCHOOL ZUID-WEST-VLAANDEREN
ASSOCIATIE K.U.LEUVEN

DEPARTEMENT LERARENOPLEIDING - RENO

Departement lerarenopleiding RENO

Sint-Jozefstraat 1
B-8820 TORHOUT

[t] 050 23 10 30
[f] 050 23 10 40
[e] reno@katho.be

Eindwerk academiejaar 2006-2007

De grootste internet-gevaren voor jongeren

Valerie Pauwelyn

o.l.v. de heer Vandewalle

Bachelor Secundair Onderwijs Handel-Burotica & Informatica

Woord vooraf

Dit eindwerk werd geschreven in het kader van mijn opleiding als bachelor secundair onderwijs waarin ik de vakkenkeuze Handel-Burotica en Informatica maakte.

Allen die mij hierbij geholpen hebben, wil ik graag bedanken.

Eerst en vooral dank ik de heer Vandewalle, informaticaleerkracht aan de Katho Reno en tevens mijn eindwerkbegeleider. Hij stond me op elk ogenblik met raad en daad bij.

Graag zou ik ook de directeur van de Katho Reno, de heer Dirk Devriendt en alle andere docenten willen bedanken voor de kansen en de begeleiding die ik via mijn lerarenopleiding kreeg. Ik betrek in mijn dank ook de mentoren die tijdens de stages hebben begeleid. Zij hebben me heel wat kennis bijgebracht.

Verder wil ik nog een welgemeend dankwoord richten aan mijn ouders en grootmoeder die me enorm steunen. Op elk moment van de dag kan ik bij hen terecht voor grote en kleine problemen. Altijd staan ze klaar met aanmoedigingen en goede raad. Ze zijn een geschenk uit de hemel.

Hartelijk dank voor alles.

De volgende computerprogramma's heb ik gebruikt om dit eindwerk te realiseren: Microsoft Office Word 2003, Microsoft Office Publisher 2003, Microsoft Internet Explorer 6.0, Microsoft Office Outlook 2003, Microsoft Outlook Express 6, Adobe Dreamweaver CS3, Nero 6 Ultra Edition en Nero 7 Premium.
Mijn werkinstrument was mijn Toshiba P20-604 laptop met een Intel Pentium 4 processor (met HT Technologie) die een kloksnelheid van 320 GHz heeft en een RAM-geheugen van 1 GB. De tv-uitzendingen werden opgenomen en op een dvd gebrand via de dvd-recorder 'DVR-520 H' van het merk Pioneer. Het volledige eindwerk werd afgedrukt met een HP All-In-One Color Laserjet 2840.

Inhoudsopgave

Inleiding

'De grootste internetgevaren voor jongeren' is het onderwerp van mijn eindwerk. Ik heb voor dit onderwerp gekozen omdat het me fascineert. Ook wil ik graag op de een of andere manier jongeren duidelijk maken welke gevaren er voor hen op het internet schuilen. Het is een hedendaagse problematiek waar mensen zich te snel bij neerleggen of er te weinig van af weten. Velen denken dat enkel de computervirussen en internetverslaving een gevaar voor het internetplezier betekenen, maar niets is minder waar.

Uit een steekproeftrekking van het Belgische I-merge en InSites Consulting kunnen we concluderen dat 72 % van de 12-jarigen tot 17-jarigen regelmatig surfen op het internet. Van de 9-jarigen tot 11-jarigen surft 43 % al regelmatig op het internet. Jongeren zitten gemiddeld 2 uur per dag op het internet. De ogen sluiten voor het internetgebruik en de internetgevaren is verleden tijd…

Uiteraard is het internet een fantastisch medium. Het is een goede manier om te communiceren met vrienden, informatie op te zoeken, een treinticket te kopen, bestanden en/of foto's te versturen, … Er zijn zoveel mogelijkheden met het internet maar velen weten niet dat ze erg moeten opletten met de persoonlijke informatie die ze over zichzelf prijsgeven. Niet iedereen op het internet heeft goede bedoelingen.

Dit eindwerk geeft een overzicht over de internetgevaren waarmee ook u geconfronteerd kunt worden. Het eindwerk heeft wel als titel 'de grootste internetgevaren voor jongeren', maar deze internetgevaren gelden in feite voor iedereen die zich op het internet waagt. Alleen vindt u in dit eindwerk niets terug over internetbankieren, physing, … want dit zijn zaken waarmee jongeren minder in contact komen. Het eindwerk is een naslagwerk dat interessant is voor ouders en leerkrachten die meer willen weten over de gevaren die jongeren en zichzelf te wachten staan in cyberspace.

Dit eindwerk bestaat uit vier grote delen. Hieronder krijgt u een idee over wat u kunt terugvinden in die delen.

1	**Deel 1: De grootste internetgevaren voor jongeren** In het eerste deel van het eindwerk worden de grootste internetgevaren voor jongeren besproken en er wordt ook bij vermeld hoe u met deze gevaren moet omgaan. U vindt er uitleg over computervirussen, spam, hackers, spyware, onveilig chatten en cyberpesten. Natuurlijk bestaan er nog andere internetgevaren waar jongeren mee geconfronteerd kunnen worden, maar de belangrijkste worden in dit eindwerk toegelicht.
2	**Deel 2: De virtuele Second Life-wereld** Dit deel geeft u een algemeen zicht over de virtuele wereld van Second Life: wat het precies is, wat u er kunt doen, welke gevaren u er kunt oplopen, … Ook de ervaringen van mijn eigen verblijf in Second Life kunt u er terugvinden.
3	**Deel 3: De Belgische wetgeving** Het derde deel van mijn eindwerk gaat over de wetgeving in verband met informaticacriminaliteit. Inbreken in een huis is volgens de Belgische wetgeving strafbaar, maar hoe zit het nu met inbreken in een computer? Een antwoord op deze vraag wordt u gegeven in het derde deel waar u ook nog andere informatie omtrent de Belgische wetgeving en informaticacriminaliteit vindt.

4

Deel 4: Bewustmaking van de internetgevaren

Als u de eerste drie delen van het eindwerk heeft gelezen, dan bent u hopelijk al een stuk wijzer geworden. Natuurlijk leest niet iedereen mijn eindwerk en ook anderen moeten ingelicht worden over de mogelijke internetgevaren. In dit gedeelte vindt u tv-uitzendingen, campagnes en artikels terug die de mensen de voorbije jaren wilden informeren over het feit dat het internet niet alleen maar rozegeur en maneschijn is. Daarnaast vindt u samenvattingen over enkele films die omtrent deze problematiek werden geregisseerd. Graag zou ik ook mijn steentje bijdragen tot de bewustmaking en heb ik een multimedia dvd gemaakt die specifiek gericht is naar jongeren (vooral van de tweede graad). Meer uitleg over dit alles vindt u dus in deel vier.

Inhoud van de eindwerkdoos

Wat vindt u naast dit eindwerk nog in de eindwerkdoos?

 *bundel papieren*	**Artikelenbundel** In deze artikelenbundel vindt u een greep uit interessante en leerrijke artikels die de laatste jaren verschenen zijn. Deze artikels hebben betrekking op enkele internetgevaren en zijn ingedeeld per thema. Een aanrader om ze eens door te nemen, want niet alle informatie die u er terugvindt, werd ook opgenomen in het theoretische gedeelte van dit eindwerk.
 *boekje*	**Ginette – Hoe ik mijn peeceefobie overwon** In het boekje 'Hoe ik mijn peeceefobie overwon' geeft Ginette tips over veilig computeren en internetten. Het boekje is vooral gericht aan volwassen computerleken, maar het is voor iedereen leuk en interessant om het eens te doorbladeren. Meer informatie over dit boekje vindt u verder terug bij het hoofdstuk campagnes.
 *dvd*	**Digitale versies & campagnefilmpjes** Op deze dvd zijn de digitale versie van het eindwerk zelf en de digitale versie van de artikelenbundel in pdf-formaat beschikbaar. Daarnaast zijn ook de campagnefilmpjes terug te vinden die vermeld zijn in het gelijknamige hoofdstuk van dit eindwerk. De campagnefilmpjes op deze dvd, kunt u enkel bekijken op de computer, niet via een dvd-speler die aangesloten is op een televisie. Inhoud van de dvd 'Digitale versies & campagnefilmpjes': 1 Eindwerk - De grootste internetgevaren voor jongeren.pdf 2 Artikelenbundel - De grootste internetgevaren voor jongeren.pdf 3 Campagnefilmpje DIGIbewust - Datingshow.wmv 4 Campagnefilmpje DIGIbewust - Zinnetjes.wmv 5 Campagnefilmpje DIGIbewust - Waar is Chris.wmv
 *dvd*	**Multimedia dvd** Deze multimedia dvd is gericht aan jongeren die willen kennismaken met de internetgevaren waar zij het meest vatbaar voor zijn. Meer informatie over deze multimedia dvd vindt u terug in het gelijknamige hoofdstuk van dit eindwerk.
	**Tv-uitzendingen (DVD 1)** Op deze dvd zijn de tv-uitzendingen terug te vinden die beschreven zijn in het gelijknamige hoofdstuk van dit eindwerk.

5

dvd

Deze dvd is zowel afspeelbaar op een computer met dvd-drive als op een dvd-speler die aangesloten is op een televisie. Via het titelmenu kunt u eenvoudig en snel navigeren tussen de verschillende tv-uitzendingen.

Inhoud van de dvd 'Tv-uitzendingen (DVD 1)':

1 Knevel & Van den Brink 14/05/2007
(Duur: 15 minuten en 48 seconden)

2 Netwerk – De digitale generatie 30/10/2005
(Duur: 29 minuten en 13 seconden)

3 Koppen – Enquête over chatten 27/03/2007
(Duur: 37 minuten en 18 seconden)

4 Het Nieuws – Cyberpedofiel 06/09/2006
(Duur: 2 minuten en 38 seconden)

5 Journaal – Cyberpedofiel 04/10/2006
(Duur: 44 seconden)

6 Panorama – De wereld van de cyberpedofielen 04/03/2007
(Duur: 41 minuten en 37 seconden)

7 Netwerk – Kinderlokkers online 09/03/2007
(Duur: 21 minuten en 43 seconden)

8 Koppen – Kinderlokkers online 05/06/2007
(Duur: 30 minuten en 11 seconden)

6

dvd

Tv-uitzendingen (DVD 2)

Op deze dvd zijn de tv-uitzendingen terug te vinden die beschreven zijn in het gelijknamige hoofdstuk van dit eindwerk.

Deze dvd is zowel afspeelbaar op een computer met dvd-drive als op een dvd-speler die aangesloten is op een televisie. Via het titelmenu kunt u eenvoudig en snel navigeren tussen de verschillende tv-uitzendingen.

Inhoud van de dvd 'Tv-uitzendingen (DVD 2)':

1 Koppen – Cyberpesten 16/03/2006
(Duur: 11 minuten en 19 seconden)

2 De Zevende Dag – Cyberpesten 26/03/2006
(Duur: 12 minuten en 30 seconden)

3 Journaal – Happy Slapping 29/09/2006
(Duur: 1 minuten en 30 seconden)

4 Panorama – Second Life 15/07/2007
(Duur: 44 minuten en 16 seconden)

5 Het Nieuws – Virtuele kinderpornografie in SL 23/03/2007
(Duur: 2 minuten en 8 seconden)

6 Netwerk – Internetverslaving 16/03/2007
(Duur: 10 minuten)

DEEL 1 DE GROOTSTE INTERNETGEVAREN VOOR JONGEREN

1 Computervirussen

1.1 Wat is een computervirus?

Een computervirus (in het dagelijks taalgebruik zegt men kortweg 'virus') is een kwaadaardig computerprogrammaatje (software). Het computervirus nestelt zich meestal ongemerkt en dus ongevraagd in uw computer. Er bestaan ontzettend veel computervirussen en elk computervirus is verschillend. Het ene computervirus kan uw computersnelheid flink vertragen terwijl een ander bijvoorbeeld al uw gegevens kan vernietigen. Niet alle computervirussen slaan onmiddellijk toe op het moment dat ze uw computer besmetten. Sommige zijn maanden op uw computer aanwezig zonder dat u er iets van merkt en dan op een bepaald moment slaan ze toe en brengen ze schade aan.

Computervirussen zijn schadelijk en de schade is afhankelijk van hun geprogrammeerde instellingen. Maar wat kan een computervirus nu precies aanrichten? Enkele voorbeelden:

- de harde schijf volzetten;
- computerprogramma's onbruikbaar maken;
- de computer onstabiel maken (bijvoorbeeld: flink vertragen);
- bestanden wijzigen;
- bestanden vernietigen;
- de harde schijf (schijven) formatteren;

Eerder werd al gezegd dat een computervirus een computerprogramma is en computerprogramma's worden door mensen gemaakt. Een computervirus is dus niet iets wat 'vanzelf' ontstaat. Computervirusschrijvers hebben diverse redenen om een computervirus te maken: om hun kennis te testen, uit wraak, voor de kick, …

Veel computervirussen zijn varianten van elkaar, maar hoe ontstaat nu zo'n variant? Wel, iemand zoekt de broncode van een bestaand computervirus op op het internet. Die persoon past de broncode wat aan en verspreidt vervolgens het computervirus. Om dergelijke broncodes te wijzigen, is er enkel wat basiskennis programmeertaal nodig.

Als een computer met een computervirus besmet wordt, dan gaat het computervirus zich op de getroffen computer vermenigvuldigen. Maar hoe gaat dat vermenigvuldigen precies in zijn werk? Dat is afhankelijk van wat de programmeur (de persoon die het computervirus heeft gemaakt) ingaf. Enkele voorbeelden:

- het computervirus kan zich verspreiden via e-mail en zo de computers van uw contactpersonen besmetten;
- het computervirus kan zich nestelen op verschillende plaatsen op uw harde schijf en kan bijvoorbeeld uw andere opslagmedia besmetten zoals een tweede harde schijf, diskette, USB-stick, …;
- het computervirus kan zich verspreiden via het netwerk naar andere computers;
- …

Door de enorme groei van het internet en de populariteit van e-mail is het aantal computervirussen de laatste jaren sterk toegenomen en worden ze ook alsmaar gemakkelijker verspreid.

1.2 De geschiedenis van het computervirus[1]

De prille geschiedenis van de computervirussen start in 1981. Toen is het allereerste experimentele computervirus 'Elk Cloner' gemaakt, dat zich verspreidde via de diskettes voor de Macintosh-computers. Het enige wat het computervirus deed, was een bericht tonen op de computer.

In 1986 werd het eerste bekende computervirus gemaakt door twee broers uit Pakistan. Zij ontdekten dat ze in de bootsector (opstartsector) van een diskette een programma konden plaatsen dat bepaalde opdrachten uitvoerde. Het eerste computervirus was geboren, en werd het 'Brain-computervirus' gedoopt. Veel deed dit eerste computervirus niet, behalve zich verspreiden op andere diskettes. Maar de kennis om een computervirus te schrijven, verspreidde zich sneller dan het computervirus zelf. Wereldwijd begonnen mensen computervirussen te schrijven, ook al was dit toen nog helemaal niet zo gemakkelijk. Men moest in machinetaal kunnen schrijven, men moest veel afweten van de hardware van computers, …

Later waagden programmeurs zich aan het schrijven van computervirussen in een gewone programmeertaal zoals C, Turbo Pascal of Basic.

Als reactie daarop zijn bedrijven gestart met het maken van anticomputervirussoftware. Dit betekende voor de meeste computervirussen dat ze geen toekomst hadden, omdat de computervirussen zich vroeger traag verspreidden, en alleen per diskette. Wanneer er een nieuw computervirus was geschreven, had de anticomputervirusfabrikant al een middeltje tegen het computervirus, nog voor het zich echt kon verspreiden.

Computervirusauteurs lieten het hier uiteraard niet bij. Ze ontwikkelden allerlei tactieken en methoden om toch de computervirusscanners te slim af te zijn. Ze plaatsten het computervirus in het RAM-geheugen, in de geheugenchips van bijvoorbeeld de videocontroller, … Men ging steeds verder en men begon zelfs computervirussen te schrijven die de anticomputervirussoftware onklaar maakten. Ook kwamen er zogenaamde stealth-computervirussen: deze computervirussen werkten zeer onopvallend, waardoor een computervirusscanner ze gewoon niet opmerkte.

In 1988 ontdekten de computervirussen ook het internet. Het eerste computervirus dat zich via het internet verspreidde, werd daarom ook 'internetworm' gedoopt. Dit legde een serieuze basis voor de vele duizenden computervirussen die hierna zouden volgen. Het 'voordeel' van het internet was dat de computervirussen heel snel konden worden verspreid, veel sneller dan diskettes.

De succesvolste computervirussen zijn echter de polymorfe computervirussen, die voor het eerst in 1991 werden geschreven. Deze computervirussen veranderen constant van 'uiterlijk'. Dit maakt het de computervirusscanner bijna onmogelijk om dit computervirus te herkennen, omdat computervirusscanners een computervirus juist herkennen aan hun 'uiterlijk'.

Vanaf 1999 werd ook, tot dan toe veilige, e-mail aangevallen, een eerste keer door het 'Melissa-computervirus', een computervirus met het vermogen om zichzelf supersnel en massaal naar iedereen ter wereld te versturen. Op dat ogenblik was dat het snelst verspreide computervirus ooit. Dit computervirus legde dan ook de basis voor vele andere computervirussen die dezelfde methode verder zouden toepassen. Ze gebruiken namelijk

---

[1] VYNCKE, P., *Veilig op het internet – De complete gids voor veilig surfen*, Lannoo, Tielt, 2005, 496 pagina's

Microsoft Outlook en Outlook Express en verspreiden zich naar de mensen die zich in het adresboek bevinden.

Hieronder volgt een overzicht van de mijlpalen voor de computervirussen:

1981	Het allereerste computervirus, Elk Cloner genaamd, wordt verspreid. Het enige wat het computervirus doet, is zich verspreiden en een tekstbericht weergeven op het scherm.
1983	Het eerste computervirus dat geschreven is voor 'onderzoek'. Dit experimentele computervirus wordt getoond op een veiligheidsseminarie. Vanaf nu worden deze programma's ook 'computervirus' genoemd, bedacht door Len Adleman.
1986	Het allereerste bootsectorcomputervirus: het Brain-computervirus, geschreven voor MS-DOS. Voor het eerst werd het programma onzichtbaar in de bootsector opgeslagen. De verspreiding begon in Pakistan.
1986	Het eerste Trojaanse paard wordt gemaakt, dat de naam PC-Write meekrijgt omdat het zich verspreidt als een shareware tekstverwerker, genaamd PC-Write.
1987	De eerste bestandcomputervirussen steken dit jaar de kop op. Ze zijn het meest geconcentreerd op de command .COM. Het eerste bestandscomputervirus is het Lehigh-computervirus.
1988	Het eerste Macintosh-computervirus verspreidt zich. Het draagt de naam MacMag.
1988	Het eerste computervirus dat uit wraak wordt geschreven. Een programmeur die werd ontslagen maakt een Macintosh-computervirus, het Scores-computervirus, dat de software die gemaakt werd door het bedrijf dat hem ontsloeg, onklaar maakte.
1988	Het eerste computervirus verspreidt zich over het internet, en wordt daarom ook internetworm genoemd. Deze worm laat over de hele wereld vele computers vastlopen. Dit is ook het eerste computervirus dat wereldwijd de krantenkoppen haalt.
1989	Het eerste Trojaanse paard dat de gegevens van de gebruiker gijzelt, doet zijn intrede. Het codeert alle informatie en vraagt vervolgens te betalen voor de coderingssleutel, zodat de gebruikers hun gegevens weer kunnen gebruiken.
1990	Het eerste computervirus-uitwisselingsplatform gaat van start in Bulgarije onder de naam VX BBS. Gebruikers kunnen hier computervirussen en hun broncode met elkaar uitwisselen, wat een serieuze impuls geeft voor de ontwikkeling van nieuwe en sterkere computervirussen. Op dat moment zijn er zo'n vijfhonderd computervirussen bekend.
1991	Het eerste polymorfe computervirus, geschreven in Zwitserland, wordt verspreid. Het computervirus verandert voortdurend van uiterlijk, waardoor het niet wordt herkend door de computervirusscanner. Er bestaan al ongeveer duizend computervirussen.

1991	Het bedrijf Symantec maakt het eerste anticomputervirusprogramma, Norton Anticomputervirus genoemd.
1992	Dit jaar haalt opnieuw een computervirus wereldwijd het nieuws: het Michelangelo-computervirus. Men waarschuwt voor enorme problemen, maar in werkelijkheid richt het maar weinig schade aan.
1992	Voor het eerst worden er programma's verspreid die het makkelijk maken om een computervirus te schrijven, bv. het Computervirus Creation Laboratory (VCL). Enkele klikken met de muis en een nieuw computervirus is gemaakt. Veel impact heeft dit niet, omdat alle 'nieuw' gemaakte computervirussen ongeveer dezelfde structuur hebben, waardoor ze in één klap allemaal onschadelijk worden gemaakt door een computervirusscanner.
1992	Het Dark Avenger Mutation Engine (DAME)-programma wordt verspreid. Dit programma kan eender welk computervirus omtoveren tot een onontdekbaar polymorf computervirus. Door de vele fouten in het programma wordt het echter weinig gebruikt. Er zijn ondertussen ongeveer tweeduizend driehonderd computervirussen bekend.
1994	Het aantal computervirussen blijft enorm toenemen en wordt inmiddels geschat op zevenduizend vijfhonderd computervirussen.
1995	Het eerste macrocomputervirus, Concept, wordt verspreid. Dit macrovirus besmet Word-documenten.
1996	Het eerste Windows 95-computervirus wordt verspreid: het Boza-computervirus.
1996	Laroux: het eerste macrocomputervirus dat Excel-bestanden besmet.
1996	Het eerste Linux-computervirus: Staog.
1996	De kaap van tienduizend bekende computervirussen wordt bereikt.
1998	Strange Brew is het eerste Java-computervirus.
1998	Het eerste Trojaanse paard dat later een wereldverspreid en veelgebruikt computervirus wordt. Het maakt het voor het eerst mogelijk om de volledige controle over te nemen van de doelcomputer op afstand via het internet.
1999	De grens van twintigduizend computervirussen wordt overschreden.
1999	Het Melissa-computervirus is het eerste computervirus dat zich verspreidt via e-mail, door gebruik te maken van het adresboek in Microsoft Outlook of Outlook Express.
1999	Tristate is het eerste macrocomputervirus dat zowel Word-, Excel- als PowerPoint-bestanden besmet.
2000	Bubbleboy, het eerste computervirus via e-mail dat zich automatisch opent bij het openen van het e-mailbericht, zonder dat er een attachment

	(bijlage) voor nodig is. Hetzelfde jaar gebruikt het 'KAK'-computervirus deze techniek om zich succesvol en massaal te kunnen verspreiden.
2000	Voor het eerst worden er DDoS-aanvallen uitgevoerd om toonaangevende websites tijdelijk onbereikbaar te maken. Slachtoffers zijn CNN, Yahoo, Amazon, eBay en nog vele anderen.
2000	In mei wordt de Love Letter het snelst verspreide computervirus tot dan toe. Het zou naar schatting voor twee tot vijftien miljoen dollar schade aangericht hebben. Het computervirus maakt enkel gebruik van huidige technieken om zich massaal te verspreiden via e-mail, maar wekt de nieuwsgierigheid van de ontvanger op door het attachment: ILoveYou.exe.
2000	Timofonica is het eerste computervirus dat het gemunt heeft op mobiele telefoons. Het valt deze aan door gesprekken te genereren vanuit een besmette computer.
2000	Het eerste computervirus dat zich richt op de Palm PDA.
2000	De grens van vijftigduizend computervirussen wordt overschreden.
2001	Het eerste computervirus dat zowel werkt op Windows als op het Linux-besturingssysteem: Winux genaamd.
2001	In mei komt ApIS te voorschijn. Het is de eerste Apple-worm die zich massaal kan verspreiden via e-mail door zich te versturen naar het hele adresboek.
2001	Het eerste PDF-computervirus, PeachyPDF-A, verspreidt zich dankzij de platformonafhankelijke PDF-documenten.
2002	LFM-926 is het eerste computervirus dat de Flash-bestanden (.swf) van Macromedia kan besmetten.
2002	Het Perrun-computervirus maakt zich bekend doordat het zich verstopt als een figuurbestand (.jpg).
2002	Het totale aantal bekende computervirussen is tachtigduizend in oktober van dit jaar.
2004	Vanaf het begin van dit jaar beginnen steeds meer computervirusschrijvers geld te zien in hun praktijken. Voor het eerst verschijnen er serieuze computervirussen die gebruikt kunnen worden om mensen te chanteren en worden gegevens van geïnfecteerde computers effectief doorverkocht. Ook worden er computervirussen in opdracht geschreven voor het bevorderen van spam en worden de adressen van de openstaande computers verkocht aan spambedrijven.
2004	Het totale aantal bekende verschillende computervirussen overschrijdt de magische grens van honderdduizend. De anticomputervirusmarkt doet het hierdoor ook zeer goed: één miljard dollar inkomsten in 2004.

1.3 Hoe verspreidt een computervirus zich?

Computervirussen kunnen zich op verschillende manieren verspreiden en kunnen dus via verschillende manieren toegang krijgen tot uw computer. Opletten is dus de boodschap!

Computervirussen kunnen zich verspreiden via:

- het world wide web (www);
- e-mail;
- een peer-to-peer netwerk;
- een netwerk;
- opslagmedia.

1.3.1 Verspreiding via het world wide web (www)

Een computervirus kan zich verspreiden via het world wide web. De laatste jaren is dit zelfs de grootste computervirusverdeler. Dit is deels te wijten aan de enorme toename van het aantal internetgebruikers en deels aan het feit dat heel veel computergebruikers continu online zijn (dankzij een breedbandverbinding), waardoor de kans op computervirusbesmetting nog groter wordt.

Er zijn verschillende manieren waarop computervirussen zich via het world wide web kunnen verspreiden, maar een webpagina op zich vormt natuurlijk geen gevaar, de objecten binnen die pagina soms wel. Zo kunt u op een bepaalde pagina een document of een programma downloaden dat een computervirus bevat. Zoals u waarschijnlijk al heeft ondervonden, zijn er veel websites die gebruik maken van ActiveX-besturingselementen die u dan moet toestaan om de website te kunnen bekijken. Vaak zijn deze ActiveX-besturingselementen ideale virusverdelers, let dus op bij welke websites u deze toestaat.

Het is dus mogelijk om via ActiveX-componenten een computervirus op uw harde schijf te installeren. Sinds de komst van Service Pack 2 voor Microsoft Windows XP, is de beveiliging hiertegen versterkt. Vroeger konden de ActiveX-componenten automatisch geïnstalleerd worden. Met de nieuwe beveiliging van Service Pack 2 verschijnt er telkens een waarschuwing als een webpagina iets wil installeren. Op die manier kunt u als gebruiker zelf beslissen of u het installeren al dan niet toelaat. Heeft u geen vertrouwen in de website die u bezoekt, dan is het beter dat u de ActiveX-besturingselementen niet installeert.

Als u goed oplet wat u bezoekt en wat u van het world wide web downloadt of installeert, dan verkleint u voor een groot stuk de risico's op computervirussen.

1.3.2 Verspreiding via e-mail

Naast het world wide web is e-mail een veel gebruikte manier om computervirussen te verspreiden. In dit geval bevindt het computervirus zich in de bijlage (attachment) van de e-mail. Indien u de afzender van een vreemde e-mail niet kent, is het beter dat u de bijlage niet opent of opslaat, want de kans dat de bijlage een computervirus bevat, is in dit geval zeer groot.

Wees alert in elke situatie want ook al kent u de afzender van het e-mailbericht, dan nog bent u niet zeker dat de bijlage 'onschuldig' is. Bepaalde computervirussen (bijvoorbeeld wormen) verspreiden zich automatisch naar alle adressen van een e-mailaccount zonder dat de computergebruiker hiervan weet heeft. Het kan dus zijn dat u een e-mail van een vriend/vriendin krijgt die een computervirus bevat, zonder dat hij/zij u een e-mail met een computervirus stuurde.

In de opsomming hieronder vindt u de meest voorkomende extensies terug die een computervirus bevatten en die doorgestuurd worden als bijlage. Natuurlijk bevatten niet alle bijlagen met een van de voorkomende extensies een computervirus en natuurlijk zijn er nog andere programma's of bestanden die een computervirus bevatten. Maar toch, …, als u een bijlage ontvangt met één van de volgende extensies is uiterste oplettendheid een noodzaak en is het zeker aan te raden om eerst het bestand of programma op computervirussen te scannen.

- .exe (extensie van een programma);
- .com (extensie van een programma of van een internationale website);
- .vbs (extensie van een Visual Basic Script);
- .scr (extensie van een screensaver);
- .pif ([Program Information File], extensie van een snelkoppeling).

1.3.3 Verspreiding via een peer-to-peer netwerk

Peer-to-peer (p2p) is het delen van bronnen, zoals bestanden, muziek, video's en programma's door middel van directe uitwisseling. Peer-to-peer maakt geen gebruik van een centrale server maar elke computer die deel uitmaakt van een dergelijk peer-to-peer netwerk staat zelf in voor het functioneren van het netwerk. Aangezien alle computers hier in directe verbinding staan met elkaar, is de kans groot dat uitgewisselde bestanden computervirussen bevatten.

Veel populaire download-programma's gebruiken deze technologie zoals KaZaA, Morpheus, BearShare, …Als u dus bijvoorbeeld (illegaal) downloadt van een dergelijk peer-to-peer netwerk, dan is het aan te raden om eerst het programma of bestand te scannen op computervirussen vooraleer u het opent.

1.3.4 Verspreiding via een netwerk

Ook via netwerken kunnen besmette bestanden worden uitgewisseld. Denk maar aan grote bedrijfsnetwerken, kantoornetwerken, netwerken op scholen,... Dergelijke netwerken kunnen soms tot duizenden computers bevatten. Wanneer één van die computers besmet raakt, kan het netwerk zeer snel volledig geïnfecteerd worden.

1.3.5 Verspreiding via opslagmedia

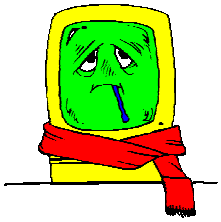
Ook als u gebruik maakt van opslagmedia is opletten de boodschap want, ook opslagmedia kunnen virusdragers zijn. Onder opslagmedia verstaan we dvd's, cd's, diskette, USB-stick, … Zo kan er een bestand of programma op het opslagmedium aanwezig zijn dat een computervirus bevat. Wees dus voorzichtig als u bestanden uitwisselt tussen verschillende computers.

Het gevaar met opslagmedia is dat u normaal gezien de persoon kent van wie de cd, diskette, usb-stick,... afkomstig is en die persoon vertrouwt. Op die manier denkt u dat er geen gevaar is voor computervirussen. Het is echter mogelijk dat de andere persoon, van wie u het opslagmedium kreeg, niet weet dat hij/zij besmette bestanden heeft op zijn/haar computer.

Het is dus aan te raden om eerst de bestanden te scannen op computervirussen vooraleer u ze van het opslagmedium naar uw computer kopieert.

1.4 Soorten computervirussen

Er werd al gezegd dat elk computervirus anders is en dat de schade verschilt van computervirus tot computervirus. Toch kunnen we de computervirussen indelen in enkele categorieën:



- bestandsvirussen;
- macrovirussen;
- bootsector- of opstartsectorvirussen;
- Trojaanse paarden;
- wormen;
- hoaxes of nepvirussen.

1.4.1 Bestandsvirussen

Een computerprogramma bestaat uit (programmeer)code en een bestandsvirus maakt daar gretig gebruik van. Een bestandsvirus koppelt een stuk code aan de (programmeer)code van een programma waardoor het desbetreffende programma besmet wordt. Wanneer de gebruiker het geïnfecteerde programma start, wordt het computervirus actief. Het bestandsvirus laadt zich in in het geheugen van de computer en gaat er op zoek naar andere actieve (geopende) programma's. Wanneer het bestandsvirus deze heeft aangetroffen, voegt het bestandsvirus ook code toe aan de (programmeer)code van deze programma's; het is een vicieuze cirkel. De gebruiker merkt niets van deze besmetting want het besmette programma werkt (voorlopig) nog normaal. Als een geïnfecteerd programma gekopieerd wordt naar een andere computer, kan het bestandsvirus ook op deze computer zijn gang gaan. Het bestandsvirus kopieert en verspreidt dus zichzelf.

De code die echter aan de (programmeer)code van de programma's wordt toegevoegd, is niet onschadelijk. De code 'doet iets': dat kan variëren van het tonen van een onschuldige tekst op het beeldscherm tot het formatteren van de harde schijven.

Bestandsvirussen zijn de meest voorkomende computervirussen.

1.4.2 Macrovirussen

Macrovirussen vormen een aparte categorie bestandsvirussen. Daarom worden ze hier apart verduidelijkt.

Macrovirussen maken misbruik van de ingebouwde programmeertaal in Microsoft Office programma's (zoals Word, Excel, …). Deze programmeertaal kunt u gebruiken om bepaalde taken (macro's) door de computer te laten uitvoeren in bijvoorbeeld een tekst, een alinea, …

Wanneer een besmet document geopend wordt of de betreffende macro wordt gestart door een nietsvermoedende gebruiker, wordt het computervirus actief. Het macrovirus richt schade aan (afhankelijk van de aard van het macrovirus) en zorgt voor de verdere verspreiding van het computervirus.

Macrovirussen vormen een steeds groter wordend probleem omdat macro's meer en meer (en zeker in de bedrijfswereld) worden gebruikt. Door het frequente gebruik worden macro's vaak automatisch toegelaten op de computer zonder dat u hiervoor toestemming moet geven. Bovendien is het eenvoudig om een macrovirus te maken of om een variant van een bestaand macrovirus te maken.

1.4.3 Bootsector- of Opstartsectorvirussen

Bootsector- of opstartsectorvirussen zijn computervirussen die zich hechten aan de (boot)code in de opstartsector van de harde schijf. Als uw computer met een dergelijk computervirus besmet wordt, dan wordt het bootsectorvirus reeds actief bij het opstarten van het besturingssysteem (bijvoorbeeld: Windows XP, Windows Vista, …) vanuit de opstartsector. Het bootsectorvirus wordt automatisch in het werkgeheugen van de computer geladen om er vervolgens zijn schadelijke werk te beginnen. Als het bootsectorvirus zich heeft ingenesteld in uw computer, dan verspreidt het zich daarna naar elke gegevensdrager (diskette, USB-stick, …) die niet schrijfbeveiligd is.

Een computer kan met een bootsectorvirus besmet worden wanneer hij bijvoorbeeld wordt opgestart met een besmette gegevensdrager (bijvoorbeeld een diskette, cd-rom). Dit kan buiten uw eigen wil zijn omdat u bijvoorbeeld de diskette bij de vorige computersessie bent vergeten te verwijderen uit uw computer.

Het besmettingsgevaar van de bootsector van de harde schijf is sterk verminderd omdat deze sector tegenwoordig vanuit het BIOS van de computer automatisch wordt beveiligd. Dit type computervirus komt ook minder en minder voor omdat het world wide web en e-mail de bovenhand hebben gekregen waardoor de verspreiding van de andere soorten computervirussen veel effectiever en sneller gaat.

1.4.4 Trojaanse paarden

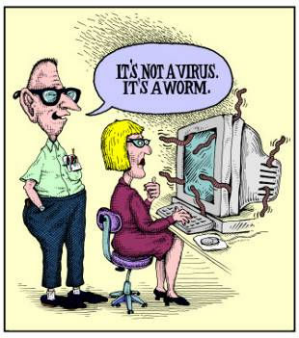
Trojaanse paarden (vaak worden ook de termen 'Trojan horses' of 'Trojans' gebruikt) zijn computerprogrammaatjes die buitenstaanders via het internet toegang verlenen tot de pc van de (nietsvermoedende) besmette gebruiker. Deze programma's zitten bijna altijd verstopt in andere programma's die u kunt downloaden van het internet, bijvoorbeeld: een mooie screensaver, een leuk spelletje, …De programma's zien er nuttig en/of leuk uit, maar ondertussen voeren ze ook verborgen spionage- of schadefuncties uit.

Veel Trojaanse paarden zijn zo ontwikkeld dat ze uw accountnaam en wachtwoord stelen en via e-mail naar iemand anders sturen (meestal naar de maker van het computervirus). Sommige Trojaanse paarden verwijderen zelfs alle gegevens van uw pc of laten af en toe vervelende meldingen zien. Maar daar blijft het niet bij…Via een Trojaans paard kan een andere gebruiker (meestal de maker van het computervirus), de besmette computer 'overnemen' via het internet. Zo kan die andere gebruiker met uw pc doen en laten wat hij/zij wil. Bekende Trojaanse paarden van dit type zijn: Netbus, Back Orifice en Sub Seven.

Technisch gezien is een Trojaans paard geen computervirus, maar het kan wel dezelfde problemen veroorzaken. Wat is nu het verschil tussen een (echt) computervirus en een Trojaans paard?

- Een Trojaans paard kan zich niet zelfstandig vermenigvuldigen of verspreiden, de meeste computervirussen verspreiden zich wel zelfstandig.
- Een Trojaans paard infecteert geen andere bestanden. Bij een computervirus is dit wel het geval.
- Een Trojaans paard verwijderen, kan simpelweg door het desbetreffende programma te verwijderen (bijvoorbeeld: de bewegende screensaver). Wilt u een computervirus verwijderen, dan heeft u een computervirusscanner nodig en dan nog loopt het verwijderen van een computervirus niet altijd van een leien dakje.

1.4.5 Wormen



Ook wormen zijn strikt genomen geen computervirussen. Een worm (de afkorting van 'write once, read many') verspreidt en vermenigvuldigt zich van computer naar computer terwijl een gewoon computervirus dit doet van bestand tot bestand. Een worm hecht zich niet aan computerprogramma's en infecteert ze ook niet. Het 'enige' wat een worm dus in feite doet, is zich verspreiden door zichzelf te kopiëren. Elke kopie maakt weer nieuwe kopieën van zichzelf die allemaal (onnodig) geheugen op de computer in beslag nemen. Het nadeel voor de gebruiker is meestal dat wormen rekentijd en geheugencapaciteit verbruiken.

Een worm vermenigvuldigt zich in een computernetwerk door gebruik te maken van de beveiligingslekken van computers. Een kopie van de worm scant het netwerk, op zoek naar andere computers met hetzelfde beveiligingslek als de besmette computer. Vervolgens kopieert de worm zichzelf naar de gevonden machines en wordt ook op deze machines het scannen gestart. Wanneer een computernetwerk een bepaald veiligheidslek heeft, dan is een worm in staat zichzelf razendsnel te vermenigvuldigen.
Naast de verspreiding via computernetwerken, bevinden wormen zich vaak in e-mail bijlagen (attachments). Als u een dergelijke bijlage opent, dan stuurt de worm zichzelf door naar alle personen uit het adresboek van uw e-mailprogramma. Dit zorgt dus voor een vicieuze cirkel.

Wormen vermenigvuldigen zich meestal onopgemerkt, hierdoor kunnen ze zich veel sneller verspreiden dan computervirussen.

1.4.6 Hoaxes of nepvirussen

Hoaxes (letterlijk vertaald (slechte) 'grappen'), ook wel nepvirussen genaamd, zijn computervirussen die geen computervirussen zijn: het zijn namelijk e-mails die valse meldingen bevatten.

Een hoax verkondigt een mededeling die in bijna alle gevallen onwaar is (hoe erg het soms ook klinkt). Maar waar kan een hoax zoal over gaan of wat kan een hoax zoal bevatten?

- Een waarschuwing dat er een erg gevaarlijk computervirus circuleert dat niet herkend wordt door antivirussoftware en die zware gevolgen heeft zoals bijvoorbeeld het formatteren van uw harde schijf. Vaak wordt ook vermeld dat de waarschuwing door een bepaald officieel of bekend bedrijf bevestigd werd (zoals bijvoorbeeld door Symantec).
- Een waarschuwing voor een computervirus dat besmettelijk is voor mensen.
- Een oproep om geld te storten of een e-mail door te sturen voor een ernstig ziek kind.
- Een bericht dat u binnen een bepaalde tijd moet doorsturen aan een bepaalde hoeveelheid mensen. Doet u dit niet, dan zal er u volgens het bericht iets ergs overkomen.
- Een bericht dat u moet doorsturen aan een bepaalde hoeveelheid mensen. Doet u dit, dan krijgt u volgens het bericht hiervoor een cadeau zoals een gsm, een mp3-speler, …
- Een mededeling dat u binnen de week voor uw hotmail-account zal moeten betalen.

- Een mededeling dat er iets kan gebeuren wanneer een vreemd nummer u een sms'je stuurt of opbelt. Dit zou als gevolg kunnen hebben dat uw gsm door hen bestuurd kan worden en/of uw telefoonrekening automatisch enorm de hoogte in schiet.
- Een waarschuwing voor de consumptie van een bepaald product: u zou een vergiftiging kunnen oplopen wanneer u bijvoorbeeld Coca-Cola drinkt.

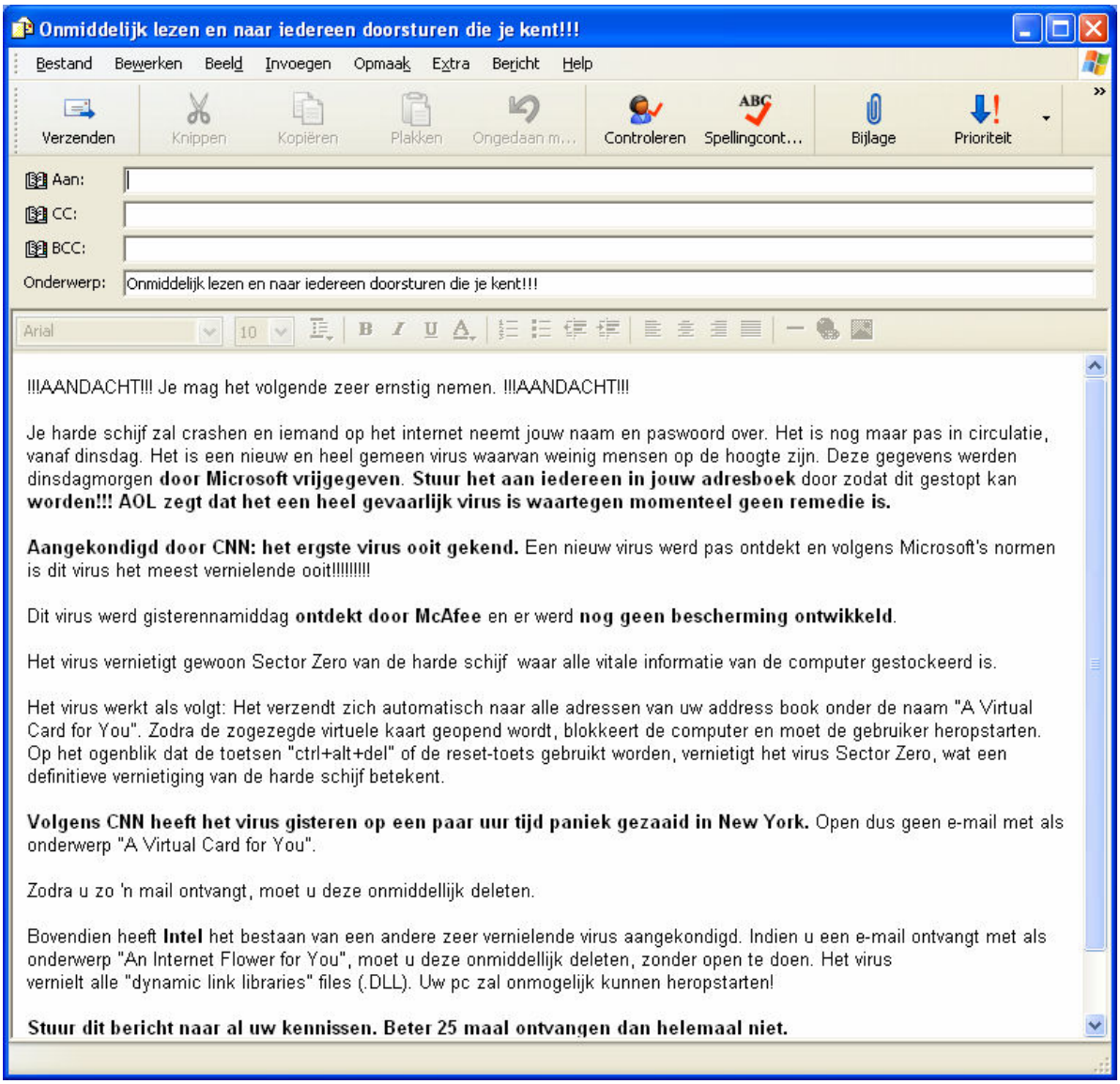
Dergelijke e-mails zijn leugens en paniekzaaierij. Bovendien vraagt men ook (altijd) om de e-mail door te sturen naar iedereen die u kent; dit is typisch voor een hoax. Dit veroorzaakt een kettingreactie en kan tot ongenoegen leiden bij de ontvangers.

Sommige mensen vinden het leuk om hoaxen te schrijven en door te sturen naar iedereen die ze kennen. Het probleem hierbij is dat veel mensen goedgelovig zijn (als het op dergelijke zaken aankomt) en de e-mail op hun beurt doorsturen naar iedereen die ze kennen. De hoax (e-mail) is immers afkomstig van een (goede) vriend(in) en hij/zij zou dit toch niet doorsturen als hij/zij wist dat er niets van aan was?

De vraag is natuurlijk hoe u weet dat een dergelijk bericht een hoax is. Met de kennis van de opsomming hierboven, herkent u in het vervolg de meeste hoaxen onmiddellijk. Het meest herkenbare van een hoax is dat men altijd in de e-mail vraagt om de e-mail door te sturen naar uw contactpersonen. U kunt ook op het internet nagaan of het al dan niet gaat om een fictief bericht. De overzichtelijkste Nederlandstalige website hiervoor is VirusAlert (http://www.virusalert.nl/?show=hoaxes).

Als u een hoax ontvangt, is het beter om deze onmiddellijk te verwijderen, ook al brengt de e-mail op zich geen schade toe. Stuur een hoax ook nooit door, want u kunt op ongenoegen stuiten bij uw contactpersonen. Het beste is ook om de afzender van de hoax (van wie u de hoax heeft ontvangen) even te laten weten dat het een hoax is en te vragen dat hij/zij dergelijke e-mailberichten in de toekomst niet meer naar u doorstuurt.

Hieronder vindt u enkele voorbeelden van hoaxen; de inhoud ervan is dus onwaar. De meest typische zaken die in hoaxen vermeld staan, werden in het vet aangeduid.



Onmiddelijk lezen en naar iedereen doorsturen die je kent!!!

Bestand Bewerken Beeld Invoegen Opmaak Extra Bericht Help

Verzenden | Knippen | Kopiëren | Plakken | Ongedaan m... | Controleren | Spellingcont... | Bijlage | Prioriteit

Aan:
CC:
BCC:
Onderwerp: Onmiddelijk lezen en naar iedereen doorsturen die je kent!!!

Arial 10

!!!AANDACHT!!! Je mag het volgende zeer ernstig nemen. !!!AANDACHT!!!

Je harde schijf zal crashen en iemand op het internet neemt jouw naam en paswoord over. Het is nog maar pas in circulatie, vanaf dinsdag. Het is een nieuw en heel gemeen virus waarvan weinig mensen op de hoogte zijn. Deze gegevens werden dinsdagmorgen **door Microsoft vrijgegeven**. **Stuur het aan iedereen in jouw adresboek** door zodat dit gestopt kan **worden!!! AOL zegt dat het een heel gevaarlijk virus is waartegen momenteel geen remedie is.**

Aangekondigd door CNN: het ergste virus ooit gekend. Een nieuw virus werd pas ontdekt en volgens Microsoft's normen is dit virus het meest vernielende ooit!!!!!!!!!

Dit virus werd gisterennamiddag **ontdekt door McAfee** en er werd **nog geen bescherming ontwikkeld**.

Het virus vernietigt gewoon Sector Zero van de harde schijf waar alle vitale informatie van de computer gestockeerd is.

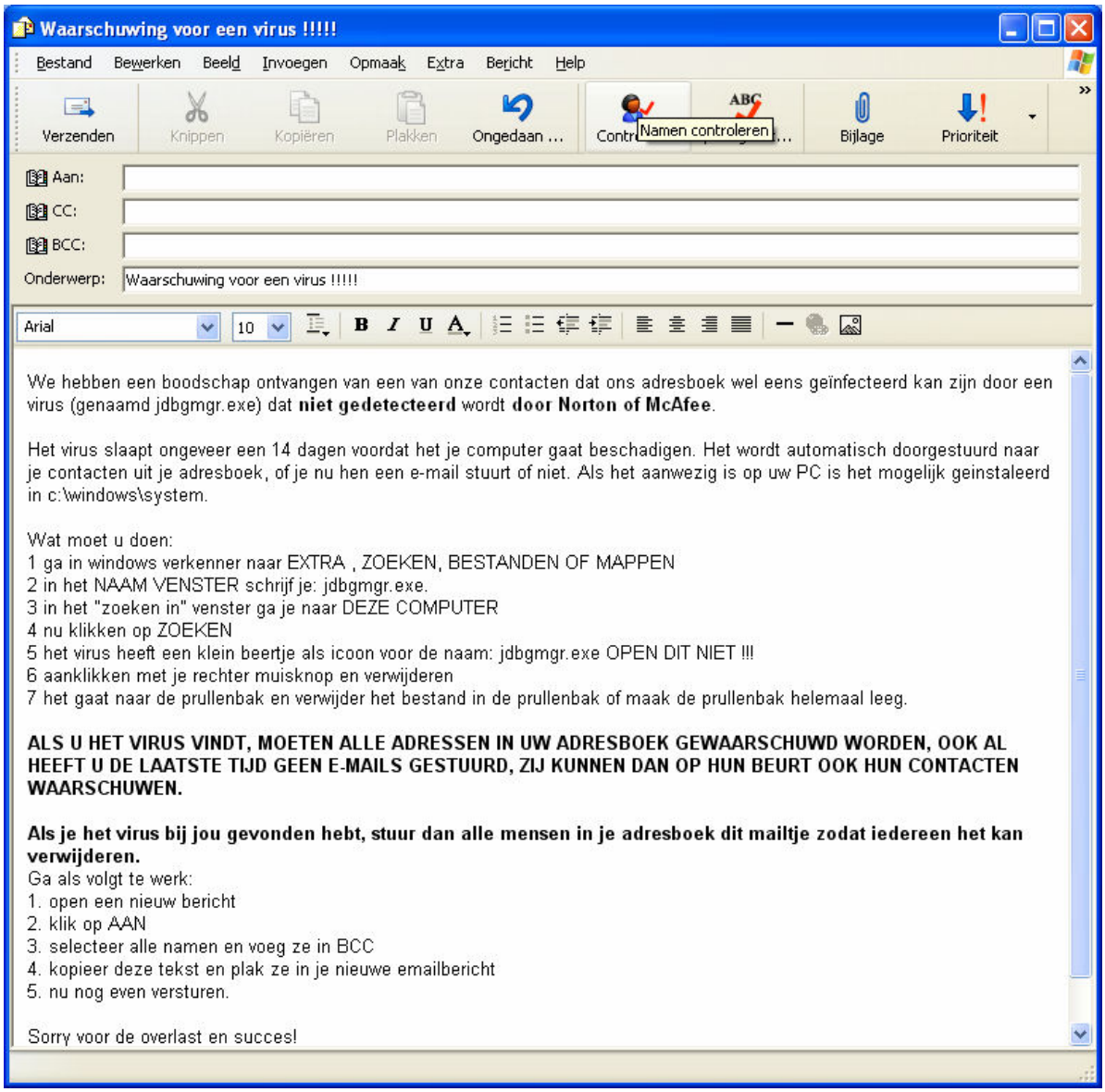
Het virus werkt als volgt: Het verzendt zich automatisch naar alle adressen van uw address book onder de naam "A Virtual Card for You". Zodra de zogezegde virtuele kaart geopend wordt, blokkeert de computer en moet de gebruiker heropstarten. Op het ogenblik dat de toetsen "ctrl+alt+del" of de reset-toets gebruikt worden, vernietigt het virus Sector Zero, wat een definitieve vernietiging van de harde schijf betekent.

Volgens CNN heeft het virus gisteren op een paar uur tijd paniek gezaaid in New York. Open dus geen e-mail met als onderwerp "A Virtual Card for You".

Zodra u zo 'n mail ontvangt, moet u deze onmiddellijk deleten.

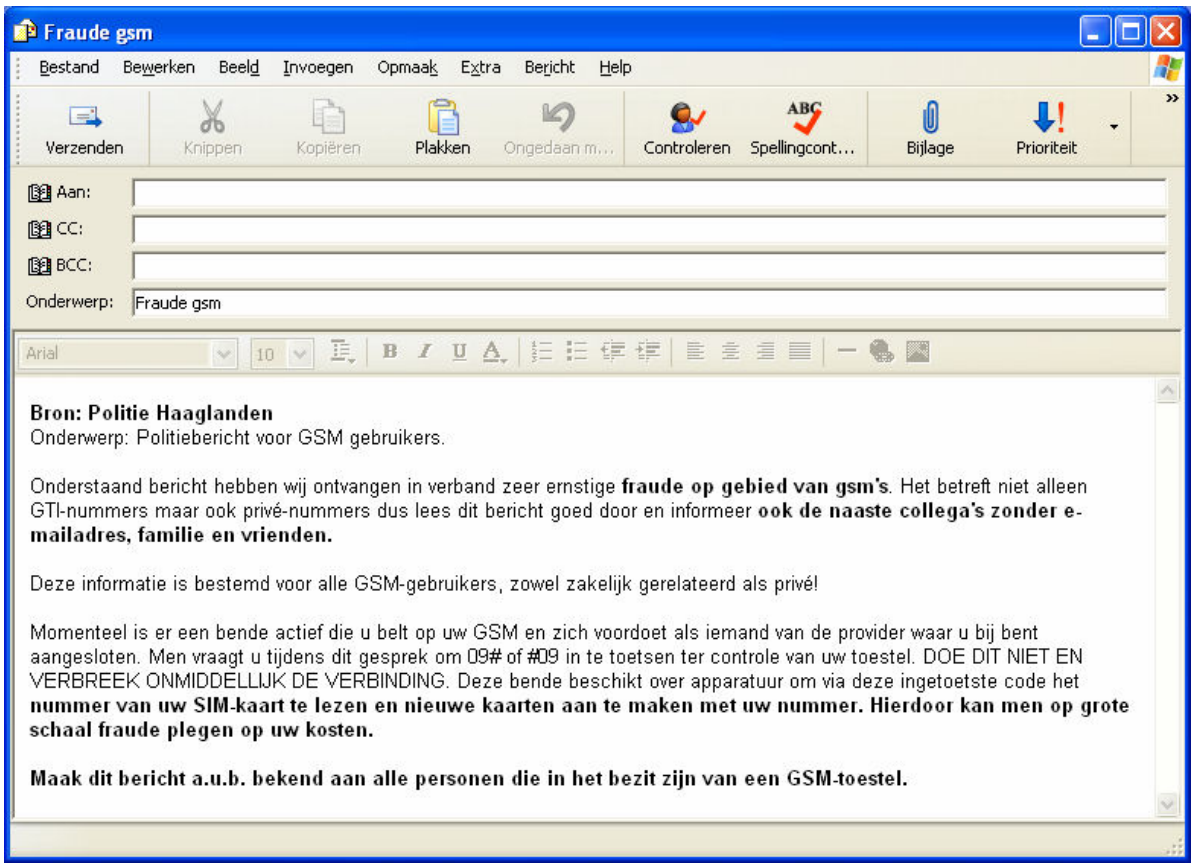
Bovendien heeft **Intel** het bestaan van een andere zeer vernielende virus aangekondigd. Indien u een e-mail ontvangt met als onderwerp "An Internet Flower for You", moet u deze onmiddellijk deleten, zonder open te doen. Het virus vernielt alle "dynamic link libraries" files (.DLL). Uw pc zal onmogelijk kunnen heropstarten!

Stuur dit bericht naar al uw kennissen. Beter 25 maal ontvangen dan helemaal niet.



Bij deze hoax wil ik toch even stilstaan omdat heel wat mensen zich hier laten beetnemen. Krijgt u deze hoax, dan is het belangrijk om onmiddellijk een e-mail te sturen naar de persoon van wie u dit bericht heeft gekregen. Verwittig deze persoon dat er geen enkele waarheid zit in dit bericht en dat hij/zij *jdbgmgr.exe* niet mag verwijderen.

Heeft u reeds dit bestand verwijderd? Kopieer dit bestand dan van uw Windows cd-rom terug naar de map *c:\windows\system*. U kunt ook vragen aan een van uw contactpersonen het bestand te zoeken op zijn/haar computer en het naar u door te sturen.


Fraude gsm
Bestand Bewerken Beeld Invoegen Opmaak Extra Bericht Help
Verzenden Knippen Kopiëren Plakken Ongedaan m... Controleren Spellingcont... Bijlage Prioriteit
Aan:
CC:
BCC:
Onderwerp: Fraude gsm
Arial 10
Bron: Politie Haaglanden
Onderwerp: Politiebericht voor GSM gebruikers.
Onderstaand bericht hebben wij ontvangen in verband zeer ernstige fraude op gebied van gsm's. Het betreft niet alleen GTI-nummers maar ook privé-nummers dus lees dit bericht goed door en informeer ook de naaste collega's zonder e-mailadres, familie en vrienden.
Deze informatie is bestemd voor alle GSM-gebruikers, zowel zakelijk gerelateerd als privé!
Momenteel is er een bende actief die u belt op uw GSM en zich voordoet als iemand van de provider waar u bij bent aangesloten. Men vraagt u tijdens dit gesprek om 09# of #09 in te toetsen ter controle van uw toestel. DOE DIT NIET EN VERBREEK ONMIDDELLIJK DE VERBINDING. Deze bende beschikt over apparatuur om via deze ingetoetste code het nummer van uw SIM-kaart te lezen en nieuwe kaarten aan te maken met uw nummer. Hierdoor kan men op grote schaal fraude plegen op uw kosten.
Maak dit bericht a.u.b. bekend aan alle personen die in het bezit zijn van een GSM-toestel.


Fantastisch voor een vriendinnenavond
Bestand Bewerken Beeld Invoegen Opmaak Extra Bericht Help
Verzenden Knippen Kopiëren Plakken Ongedaan ... Controleren Spellingcont... Bijlage Prioriteit
Aan:
CC:
BCC:
Onderwerp: Fantastisch voor een vriendinnenavond
Arial 10
Wij van libresse houden een eenmalige actie Voor alle meiden die graag en vaak libresse gebruiken, hebben we nu een verassing om wat terug te doen!! Libresse, geeft nu, HELEMAAL GRATIS make- up setten weg!!! Met lippenstift in 3 verschillende kleuren, zwarte mascara, lippotlood, blauw en roze oogschaduw, en lipgloss!! Alles wat je moet doen is deze mail minstens naar 10 vriendinnen door te sturen, en je krijgt een gratis make-up set thuis bezorgd!
Maak een kopietje van dit mailtje, en stuur dit naar: libresse@amsterdam.nl
Stuur ook je naam en adres mee, anders kunnen wij het make-up setje NIET bezorgen! Naar hoe meer mensen je dit mailtje doorstuurt, des te meer komt er bij het make up setje!! normale setje dat hierboven al is beschreven.
15 mensen: het normale setje + glittters!
20 mensen: het normale setje + glitters + parfum van nafnaf
[Voornaam + Naam]
[Straatnaam + Nummer]
[Postcode + Gemeente]

1.5 Hulpmiddelen om computervirussen te verbannen

Een computervirus is altijd schadelijk, maar het ene is al schadelijker dan het andere. Volgens experts zijn er al meer dan honderdentwaalfduizend computervirussen in omloop en komen er dagelijks ongeveer vijfentwintig bij. De kans dat ook u ooit een 'aanval' van een computervirus krijgt, is zeer groot. Het is geen overbodige luxe om uw computer tegen dergelijke aanvallen te beveiligen; zo kan een computervirus tegengehouden worden vooraleer het uw computer besmet. Is uw computer toch door een of ander computervirus besmet, dan moet u zeer voorzichtig te werk gaan. Bij het verwijderen van een computervirus loopt u immers het risico om uw gegevens en/of programma's te beschadigen.

Er bestaan verschillende hulpmiddelen om computervirussen tegen te houden wanneer ze uw computer willen binnendringen en/of om computervirussen te verwijderen wanneer ze zich al genesteld hebben in uw computer:

- antivirusprogramma's;
- online virusscanners;
- removal tools;
- antivirus door uw provider.

1.5.1 Antivirusprogramma's

Computervirussen hebben alleen maar nadelen en het is dan ook belangrijk dat u uw computer hiertegen beschermt. Een goed antivirusprogramma is daar het ideale hulpmiddel voor.

Een antivirusprogramma, ook wel antivirussoftware of virusscanner genaamd, is een computerprogramma dat uw computer probeert te beschermen tegen computervirussen en dat computervirussen verwijdert. Het heeft twee specifieke opsporingsmethoden om computervirussen te zoeken: de on-demand scans en de on-access scans.

Dagelijks worden er ongeveer vijfentwintig nieuwe computervirussen aangemaakt. Het is dan ook belangrijk dat het antivirusprogramma regelmatig geüpdatet wordt zodat het op de hoogte is van de nieuwe computervirussen en weet hoe ze te bestrijden. Uw computervirusscanner elke dag updaten is geen overbodige luxe. U kunt er ook voor zorgen dat het antivirusprogramma zichzelf op vooraf ingestelde tijdstippen update.

Er bestaan heel wat antivirusprogramma's, het ene al wat degelijker dan het andere. De meeste antivirusprogramma's zijn betalend, al bestaan er ook enkele goede gratis virusscanners. Enkele bekende virusscanners op een rijtje:

- Norton Antivirus (http://www.norton.com);
- F-Secure (http://www.f-secure .com);
- Panda (http://www.pandasoftware.com);
- McAfee (http://www.mcafee.com);
- F-PROT (http://www.f-prot.com);
- Antivir (http://www.free-av.com) ⇨ gratis antivirusprogramma;
- AVG (http://www.grisoft.com) ⇨ gratis antivirusprogramma.

1.5.1.1 De opsporingsmethode on-demand scan

Elke computervirusscanner heeft een on-demand gedeelte. Het is hierbij de bedoeling dat u zelf de opdracht geeft om op een willekeurig tijdstip op zoek te gaan naar computervirussen. Als gebruiker kunt u opteren om de volledige harde schijf, een bepaalde partitie, een bepaalde map of een bepaald bestand te scannen op computervirussen.

Een on-demand scan moet dus door de gebruiker zelf gestart worden. De meeste virusscanners beschikken over een planner, waarbij de gebruiker bepaalde tijdstippen kan instellen waarop de computervirusscan automatisch moet starten. Handig voor wie wat vergeetachtig is.

Tip: laat op regelmatige basis de volledige computer scannen op computervirussen. Er zijn namelijk computervirussen die toch door de mazen van het net glippen en bij een virusscan gevat kunnen worden. Het is aan te raden om een volledige scan toch één keer per week uit te voeren. U doet dit best wanneer u de pc niet nodig heeft want een volledige virusscan kan lang duren en vertraagt sterk uw computer (op dat moment).

Vindt de computervirusscanner een computervirus tijdens de on-demand scan, dan zal hij proberen het computervirus uit het bestand te verwijderen. Lukt dit niet, dan zal het antivirusprogramma proberen om het computervirus in het bestand onschadelijk te maken.

De bedoeling van de on-demand scan is vooral om eventueel reeds actieve computervirussen op te sporen en te verwijderen.

1.5.1.2 De opsporingsmethode on-access (real-time) scan

De on-access scan of ook wel de real-time scan genaamd, draait op de achtergrond en controleert al het in- en uitgaand verkeer. Elk bestand dat op de computer binnenkomt en elk bestand dat van de computer vertrekt, wordt door de virusscanner gecontroleerd. Inkomende bestanden zijn bijvoorbeeld documenten die vanaf een cd-r(w), dvd-r(w), diskette, memory-stick gekopieerd worden naar de harde schijf. Ook e-mails die ontvangen worden, bestanden die gedownload worden, …worden gescand.

Deze real-time controle gebeurt door middel van een database met signaturen. Elk computervirus heeft een bepaalde signatuur. Wanneer de scanner merkt dat een inkomend bestand een signatuur heeft die overeenkomt met een signatuur uit de database, dan weet hij dat het om een computervirus gaat en zal hij tot actie overgaan. Wat er precies gebeurt, hangt af van de instellingen van de virusscanner. In de meeste gevallen zal geprobeerd worden om het bestand te verwijderen.

De bedoeling van de on-access scan is vooral om infectie van de computer te voorkomen.

1.5.1.3 De installatie van een antivirusprogramma

Hieronder wordt uitgelegd hoe u een antivirusprogramma kunt installeren. We verduidelijken dit via het gratis antivirusprogramma AVG. De installatie van andere antivirusprogramma's is gelijkaardig.

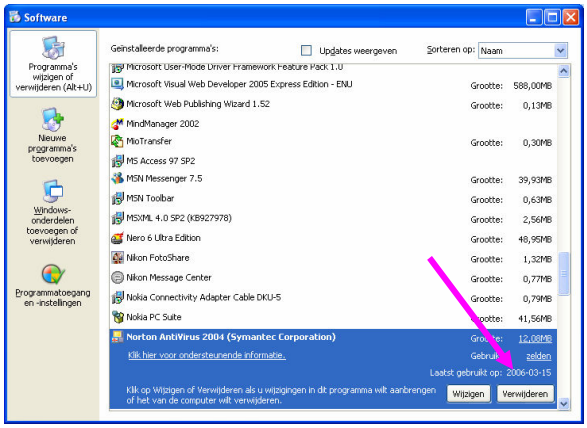
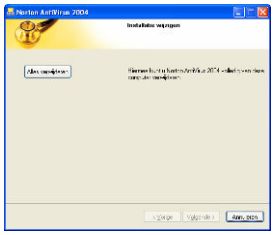
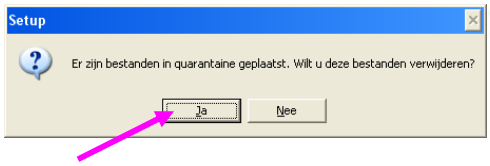
Heeft u al een goed werkend antivirusprogramma? Laat dan dit puntje over. Het puntje 'de installatie van een antivirusprogramma' is namelijk bedoeld voor mensen die nog geen antivirusprogramma hebben of waarvan hun antivirusprogramma niet meer bruikbaar is (bij het merendeel van de betalende versies is er bijvoorbeeld een gelimiteerde gebruiksduur). Heeft u echter twee of meer antivirusprogramma's op uw computer staan, verwijder dan één van deze twee antivirusprogramma's. Twee of meer antivirusprogramma's zijn niet veiliger dan één goede virusscanner, want ze zorgen voor een tragere computer en kunnen problemen veroorzaken doordat ze onderling concurrentie gaan voeren.

Volgende zaken komen hieronder aan bod:
- voorgaande antivirusprogramma('s) verwijderen;
- het antivirusprogramma AVG downloaden;

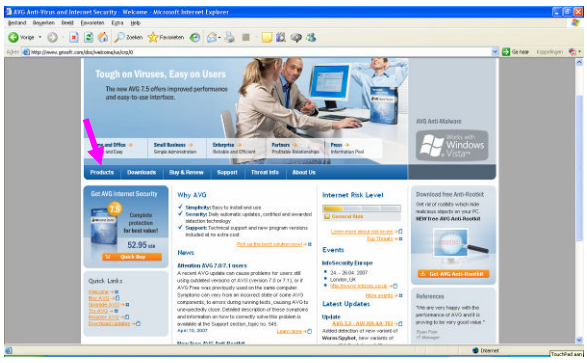
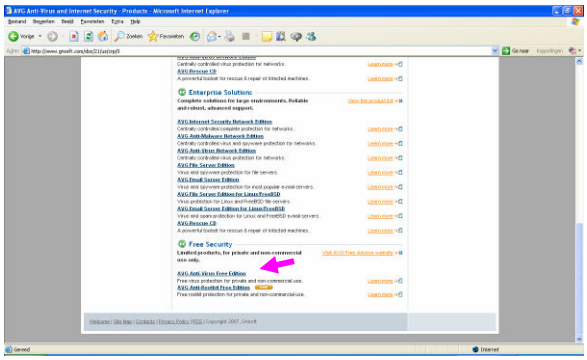
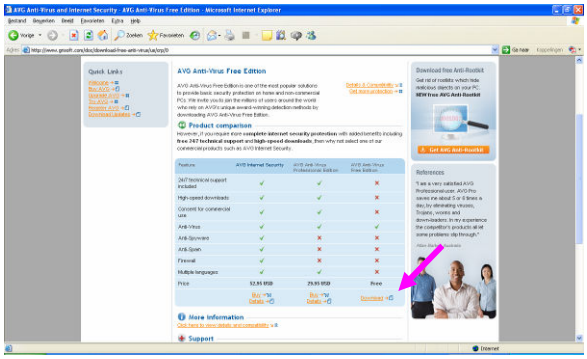
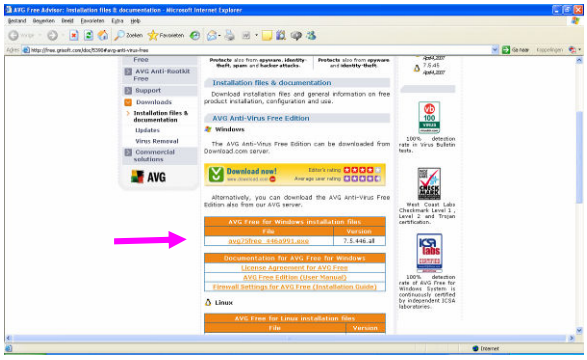
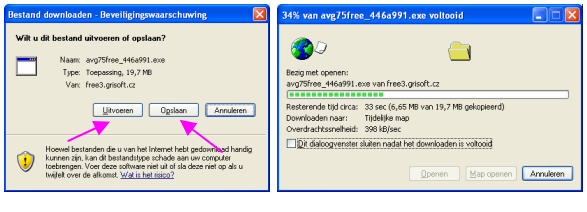
- het antivirusprogramma AVG configureren voor gebruik;
- het antivirusprogramma AVG gebruiken.

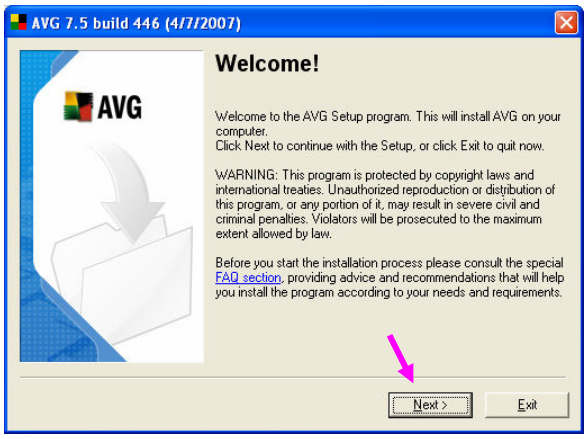
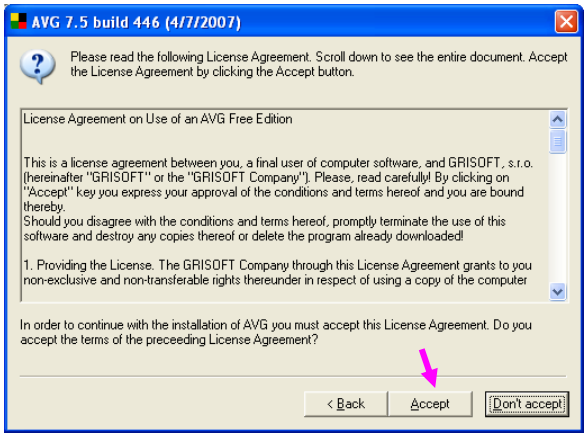
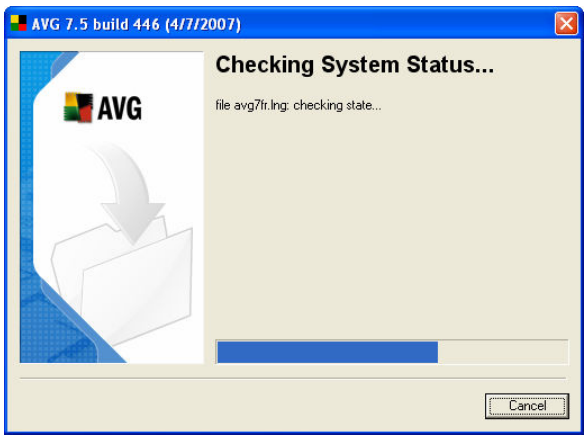
1.5.1.3.1 Voorgaande antivirusprogramma('s) verwijderen

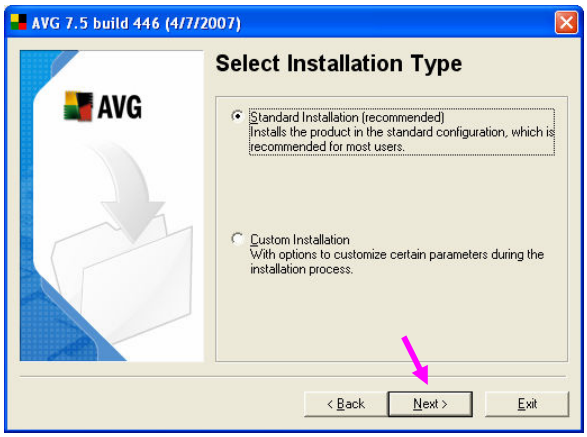
Voor u aan de installatie van een nieuw antivirusprogramma begint, moet u eerst alle voorgaande antivirusprogramma's van uw computer verwijderen. Dit doet u enkel en alleen door de onderstaande stappen te volgen. Herneem deze stappen totdat alle antivirusprogramma's van uw computer verwijderd zijn.

 	Sluit alle openstaande documenten en actieve programma's. Als uw antivirusprogramma actief is, moet u dit ook uitschakelen. Ga naar *Start*, *Configuratiescherm*.
	Kies voor de categorie *Software.*
	In het venster *Software* moet u op zoek naar de naam van het antivirusprogramma dat u wilt verwijderen. U selecteert de naam en klikt op de bijhorende knop *Verwijderen.* In mijn geval wil ik *Norton Antivirus 2004* verwijderen.
   	Wat nu volgt, is afhankelijk van antivirusprogramma tot antivirusprogramma. Doorloop de stappen van de wizard van uw eigen antivirusprogramma en kies ervoor om alles te verwijderen. Als de setup vraagt om de bestanden die in quarantaine geplaatst werden te verwijderen, dan kiest u het best voor de optie *Ja.* Na het verwijderen zal de computer vragen om opnieuw op te starten, ga dan ook op deze vraag in.

1.5.1.3.2 Het antivirusprogramma AVG downloaden

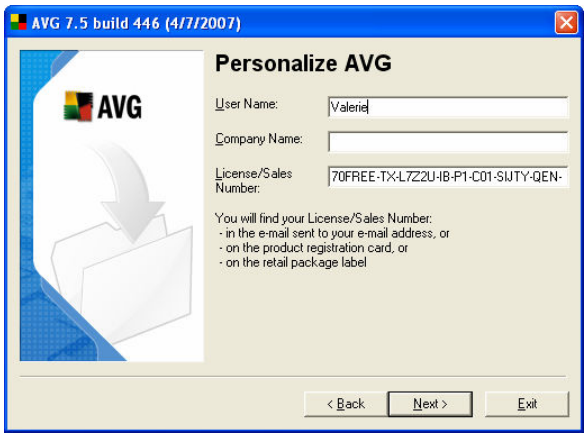
AVG	Surf naar de website http://www.grisoft.com
	Klik op de hyperlink *Products*.
	Scrol naar helemaal onderaan de webpagina. Onder het deeltje *Free Security* klikt u op de hyperlink *AVG Anti-virus Free Edition.*
	Klik bij de derde optie '*AVG Anti-virus Free Edition'* op *Download.*
 	Indien u werkt onder het besturingssysteem *Windows,* klik dan op het '*AVG Free for Windows installation file'.* Als u een beveiligingswaarschuwing krijgt, klik dan op de knop *Uitvoeren* of *Opslaan.* Kiest u voor de optie *Uitvoeren* dan wordt het installatiebestand slechts tijdelijk opgeslagen op de computer. Kiest u voor de optie *Opslaan* dan kunt u een locatie opgeven om het installatiebestand permanent op uw computer op te slaan (totdat u het zelf verwijdert). U mag kiezen welke optie u verkiest. Ik kies voor de optie *Uitvoeren.* Vervolgens wordt het antivirusprogramma

	gedownload. Als u nog een beveiligingswaarschuwing krijgt, mag u in dit geval klikken op de knop *Uitvoeren.*
	De wizard om het antivirusprogramma te installeren, wordt gestart. Klik op de knop *Next* om verder te gaan met de wizard.
	Lees de licentieovereenkomst. Gaat u akkoord, klik dan op de knop *Accept*. Gaat u niet akkoord met de licentieovereenkomst dan klikt u op de knop *Don't accept* waardoor de installatie wordt afgebroken. Ik ga akkoord met de licentieovereenkomst en klik op de knop *Accept*.
	Tijdens de derde stap van de wizard wordt de status van het systeem gecontroleerd. Dit neemt ongeveer een minuutje in beslag.



In de volgende stap vraagt men om te kiezen voor een standaardinstallatie of voor een aangepaste installatie. U moet het gewenste keuzebolletje aanstippen.

Ik laat de optie voor de standaardinstallatie staan en klik op de knop *Next.*



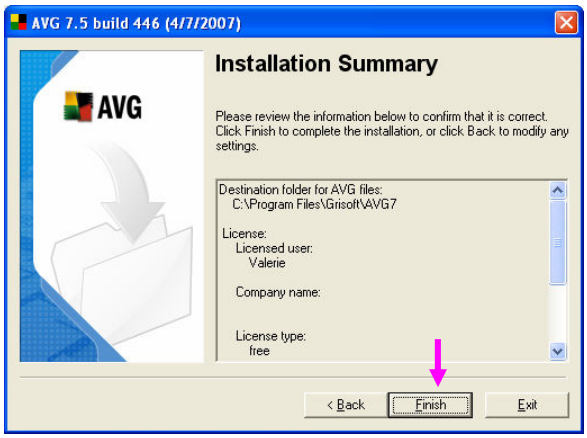
De vijfde stap van de wizard vraagt om een gebruikersnaam en een bedrijfsnaam.

Vul bij *User Name* een eigen gebruikersnaam in (bijvoorbeeld: Valerie)

Ik laat het veld bij *Company Name* (bedrijfsnaam) leeg omdat ik een thuisgebruiker ben.

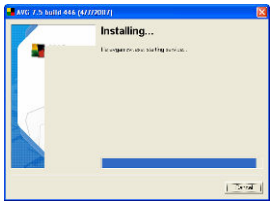
Het licentienummer werd automatisch door de wizard ingevuld.

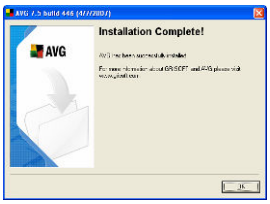
Bevestig deze invoer door op de knop *Next* te klikken.



Vervolgens krijgt u een samenvatting van de installatie.

Klik op de knop *Finish.*





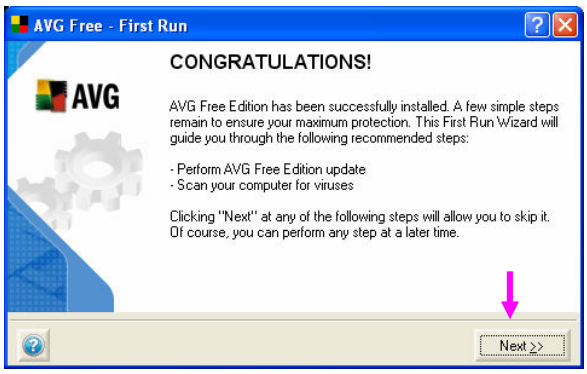
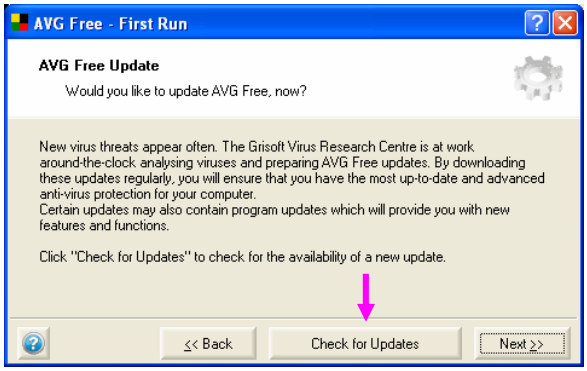
Vervolgens wordt het antivirusprogramma geïnstalleerd op de computer.

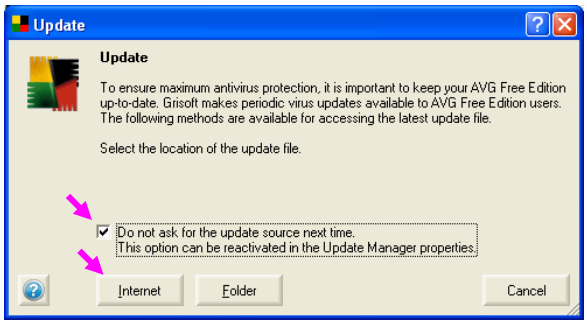
Daarna verschijnt er automatisch een volgend venster dat weergeeft dat de installatie voltooid is.

Sluit de wizard af door op de knop *OK* te klikken.

1.5.1.3.3 Het antivirusprogramma AVG configureren voor gebruik

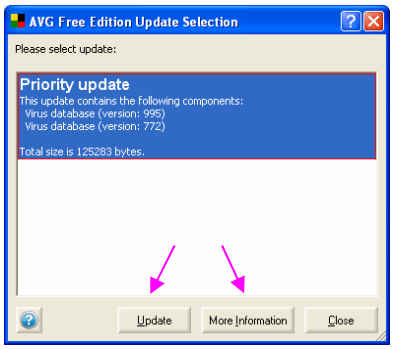
Nadat de installatie voltooid is, wordt AVG automatisch gestart. De eerste keer dat AVG gestart wordt, moet u een *First Run* doorlopen om bepaalde instellingen te bepalen.

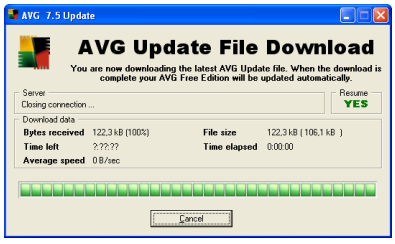
<table>
<tr>
<td> 
</td>
<td>AVG wordt automatisch gestart. U krijgt meteen een welkomstvenster.
Klik op de knop Next om verder te gaan.</td>
</tr>
<tr>
<td> 


</td>
<td>Bij de tweede stap kunt u uw antivirusprogamma updaten. Klik hiervoor op de knop Check for Updates.

Er wordt een dialoogvenster weergegeven. Er wordt vermeld dat AVG periodiek virusupdates doet om de maximale bescherming te bevorderen. Men vraagt waar men die virusupdates moet gaan halen: van het internet (optie Internet) of van een bepaalde map of gegevensdrager (optie Folder).

Indien u het vinkje aanvinkt 'Do not ask for the update source next time' zal men het internet altijd als locatie gebruiken om computervirusupdates af te halen tenzij u dit wijzigt.

Vink deze optie aan en klik op Internet.</td>
</tr>
<tr>
<td> 


</td>
<td>Er verschijnt een nieuw venster met de update(s) die beschikbaar is (zijn). U selecteert de update.

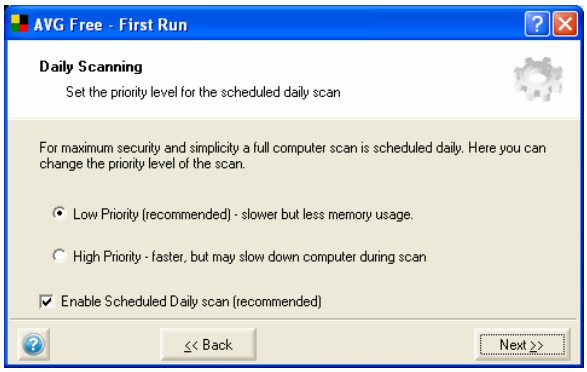
Wilt u meer informatie over de geselecteerde update dan kunt u klikken op de knop More Information.

Ik wil de geselecteerde update uitvoeren en klikken op de knop Update.

Ik krijg vervolgens een venster dat de voortgang van het downloaden (van de update) weergeeft.

Als de update succesvol is geïnstalleerd krijgt u een berichtvenster dat u moet bevestigen door op OK te klikken.</td>
</tr>
</table>

U keert automatisch terug naar stap twee van de wizard *'First Run'*. Klik op de knop *Next* om de wizard verder te doorlopen.

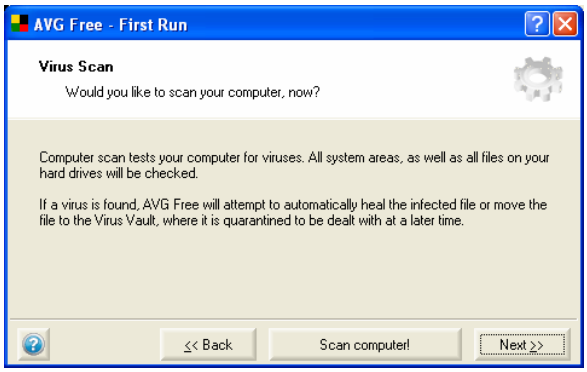


Bij deze stap van de wizard kunt u het dagelijks scannen naar computervirussen instellen.

Als u de optie '*Low Priority*' aanstipt, wordt er dagelijks traag gescand naar computervirussen. Dit verbruikt minder geheugen dan de tweede optie.
Kiest u de optie '*High Priority*', dan wordt er dagelijks snel naar computervirussen gescand maar kan tijdens het scannen de computer vertragen.

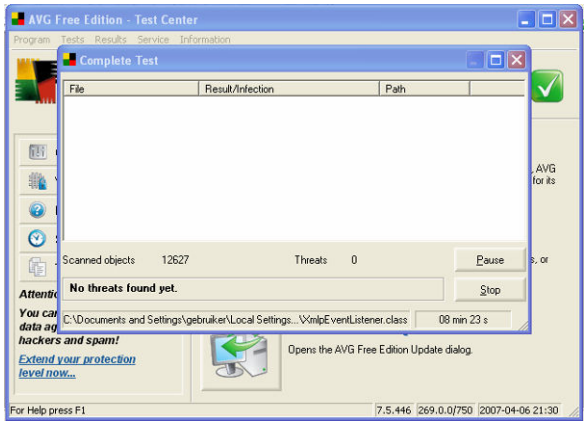
Het selectievinkje is automatisch ingeschakeld bij de optie '*Enable Sheduled Daily Scan*'. Schakelt u dit vinkje uit, dan schakelt u het dagelijkse scannen uit.

Kies tussen de opties '*Low Priority*' en '*High Priority*' en laat het vinkje ongewijzigd.
Klik na uw keuze op de knop *Next.*



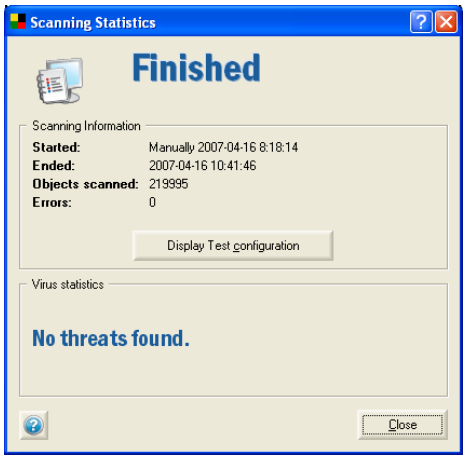
Bij de vierde stap van de wizard wordt er gevraagd of u uw computer nu wilt laten scannen.

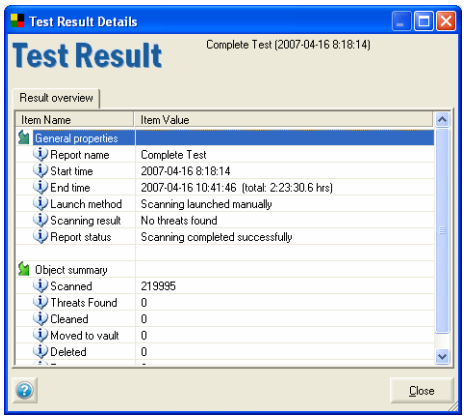
U laat uw computer scannen op computervirussen door op de knop *Scan computer* te klikken.



Er wordt een venster geopend dat de voortgang van het scannen toont: hoeveel objecten er reeds werden gescand, hoelang men al aan het scannen is en hoeveel besmette bestanden men al gevonden heeft.

In dit venster heeft u ook de mogelijkheid om het scannen te pauzeren of te stoppen.



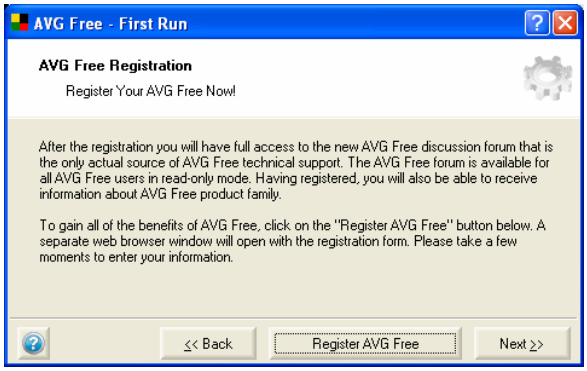


Als de volledige computer gescand werd, krijgt u een bericht met de vermelding 'Finished' en of de virusscanner al dan niet een computervirus gevonden heeft.

In dit geval werd er geen computervirus aangetroffen.

Wanneer u op de knop *Close* klikt, krijgt u een nieuw venster met de testresultaten zoals de tijdsduur, wat er gescand werd, hoeveel computervirussen er verwijderd werden, …

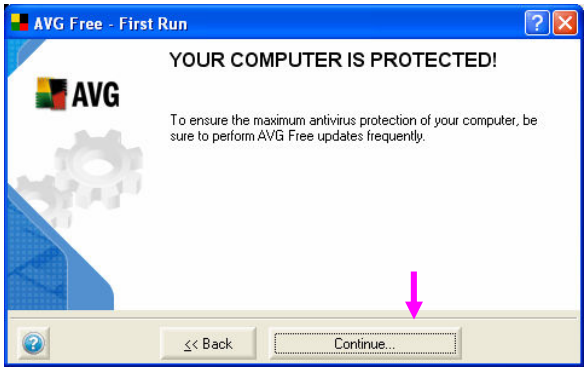
Klik ook bij dit venster (na het overlopen van de testresultaten) op de knop *Close.* U keert terug naar de wizard 'Fast Run'.



In de volgende stap van de wizard kunt u ervoor opteren om uw AVG-virusscanner te registreren. Volgens AVG haalt u alleen maar voordelen uit uw registratie.

Klik op de knop *Register AVG Free* om naar de registratiepagina te gaan. Vul er de gevraagde gegevens in.

Wilt u zich niet registreren, klik dan op de knop *Next*.



Vervolgens krijgt u de laatste stap van de wizard '*First Run'* voorgeschoteld.

Het bericht geeft weer dat uw computer beschermd wordt en dat u regelmatig uw virusscanner moet updaten.

Klik op de knop *Continue…* om de wizard te beëindigen.

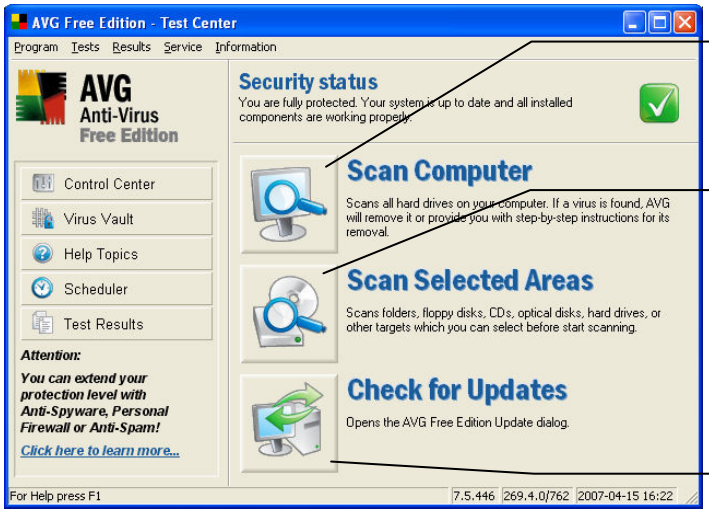
Het antivirusprogramma beschermt uw computer nu tegen virusaanvallen. U kunt zien dat de virusscanner actief is doordat het logootje van AVG in de taakbalk staat.

1.5.1.3.4 Het antivirusprogramma AVG gebruiken

Met een gratis versie van een programma heeft u natuurlijk niet altijd dezelfde mogelijkheden als bij een betalende versie; dit is niet anders bij AVG. Zo heeft u bij de gratis versie van AVG bijvoorbeeld niet de mogelijkheid om zelf bepaalde tijdstippen te plannen waarop de computer moet scannen of de software moet gaan updaten. Maar het belangrijkste en het hoofddoel van een virusscanner biedt AVG zonder problemen ook aan bij de gratis versie: mogelijkheid om computer, bestanden, … te scannen op computervirussen en de virusscanner te updaten.

Als AVG een computervirus vindt, zal het het computervirus verwijderen of u stap-per-stap begeleiden om het computervirus te verwijderen.

Open het testcenter van de virusscanner via *Start, Alle programma's, AVG 7.5, AVG Test Center.* De mogelijkheden worden even kort verduidelijkt.



Als u hierop klikt, worden alle harde schijven van de computer gescand.

Als u hierop klikt, kunt u kiezen welke media u wilt scannen. Zo kunt u bijvoorbeeld uw diskette en uw USB-stick, een bepaalde map, … laten scannen op computervirussen.

Als u hierop klikt, wordt er gezocht naar nieuwe updates van de virusscanner.

Vindt u een bepaald bestand of bestandsmap verdacht, klik dan rechts op het bestand of op de map en kies in het snelmenu voor *Scan with AVG*. Het bestand of de map wordt gescand op computervirussen en het resultaat wordt u getoond. Als de virusscan positief is, kunt u met een 'gerust' hart verder werken.

1.5.2 Online virusscanners

Indien u een 'second opinion' wenst om zeker te zijn dat de computer virusvrij is of als u nog geen computervirusscanner op de computer heeft geïnstalleerd, dan kunt u gebruik maken van een online virusscanner. Een online virusscanner scant uw computer op computervirussen vanop het internet. Er wordt dus geen virusscanner gedownload op uw computer.

Een online virusscanner kan enkel on-demand scannen en kan dus geen on-access scans uitvoeren.

Hieronder vindt u een selectie van enkele bekende online virusscanners. Omdat deze scanners gebruik maken van ActiveX-technologie, is het enkel mogelijk om deze via de browser Microsoft Internet Explorer te gebruiken.

	Panda Active Scan Mogelijkheden: • Scant, desinfecteert en verwijdert meer dan 90 000 computervirussen, wormen en Trojaanse paarden. • Scant in alle systeemapparaten, harde schijven, gecomprimeerde bestanden en e-mail mappen. • Wordt minstens eenmaal per dag geüpdatet. Internetadres: http://www.pandasoftware.com/products/activescan.htm
	Trend Micro HouseCall Mogelijkheden: • Mogelijkheid om te kiezen welke schijven en/of mappen gescand worden. • Geïnfecteerde bestanden kunnen hersteld en verwijderd worden. Internetadres: http://nl.trendmicro-europe.com/consumer/housecall/housecall_launch.php
	BitDefender Online Scanner Mogelijkheden: • Scant het geheugen, alle bestanden, mappen en de bootsector van de harde schijf. • U kunt ook optioneel scannen in gecomprimeerde bestanden, geheugen, e-mail en netwerk harde schijven. • Scant op meer dan tienduizend computervirussen, wormen, Trojaanse paarden en andere. Internetadres: http://www.bitdefender.com/scan8/ie.html
	McAfee FreeScan Mogelijkheden: • Gebruikt de McAfee ComputervirusScan Engine. • Heeft niet de mogelijkheid om computervirussen te verwijderen. Er wordt enkel een overzicht gegeven van de geïnfecteerde bestanden en informatie over hoe u deze kunt verwijderen. • Registratie is verplicht alvorens u van deze dienst gebruik kunt maken. Internetadres: http://us.mcafee.com/root/mfs/

1.5.3 Removal tools

Het kan gebeuren dat een bepaalde virusscanner een computervirus detecteert, maar er niet in slaagt om het computervirus te verwijderen. In deze situatie is een removal tool het ideale hulpmiddel om het computervirus van uw computer te verbannen.

Een removal tool is een programmaatje dat ervoor zorgt dat een bepaald computervirus van de computer verwijderd wordt. Wilt u een bepaald computervirus met een removal tool verwijderen, dan moet u een specifieke removal tool voor dat computervirus gaan downloaden en uitvoeren. Deze removal tools zijn computervirusspecifiek en kunnen dus niet voor het verwijderen van een ander computervirus gebruikt worden. Het is als een soort mini-antivirusprogramma dat slechts één enkel computervirus herkent en verwijdert.

Een removal tool downloadt u het best van websites van gerenommeerde antivirusfabrikanten. Downloadt u een removal tool van een onbetrouwbare (vreemde) website dan kan die misschien zelf wel een computervirus bevatten. Meestal wordt een removal tool niet lang na het ontstaan van een nieuw computervirus gepubliceerd en die zijn doorgaans gratis te downloaden.

Hieronder volgt een overzichtje met enkele 'veilige' internetadressen waar removal tools te vinden zijn. Natuurlijk zijn er nog heel wat andere betrouwbare websites die removal tools aanbieden.

symantec.	Internetadres: http://www.symantec.com/enterprise/security_response/removaltools.jsp
F-SECURE	Internetadres: http://www.f-secure.com/download-purchase/tools.shtml
KASPERSKY ANTI-VIRUS	Internetadres: http://www.kaspersky.com/removaltools

1.5.4 Antivirus door uw provider

De meeste providers voeren gratis een virusscan uit op de e-mails van hun klanten. Op deze manier zorgt men ervoor dat alle e-mails, die u ontvangt op het e-mailadres van uw provider, automatisch eerst gescand worden op computervirussen. Alle bekende computervirussen worden door deze virusscanner verwijderd vóór ze uw computer bereiken.

Let wel: de virusscanner van uw provider houdt niet alle computervirussen tegen. Het is een nuttig extraatje (een extra service) maar kan niet de virusscanner vervangen op uw eigen computer. Vertrouw dus niet enkel en alleen op de virusscanner van uw provider.

1.6 Werd mijn computer besmet met een computervirus?[1]

Bij een lichamelijke ziekte kan uiteindelijk enkel de dokter vaststellen of u daadwerkelijk ziek bent en wat u juist heeft. Bij de computer is het uiteindelijk de virusscanner die aangeeft of de pc besmet is met een computervirus en zo ja, met welk computervirus.

Bij een ziekte vertoont u natuurlijk meestal ook bepaalde symptomen, waaruit u zelf kunt afleiden of u ziek bent en misschien zelfs wat er precies aan de hand is. Bij de computer is dit niet anders: er zijn meestal een reeks symptomen die kunnen wijzen op een computervirus. Let op: uw computer is niet altijd 'ziek' indien één of meer van deze symptomen voorkomen, het probleem kan ook een andere oorzaak hebben. Bovendien is het zo dat uw computer niet per definitie virusvrij is omdat hij geen van deze symptomen heeft. Net zoals in het echte leven vertonen we niet altijd (onmiddellijk) symptomen terwijl we toch besmet zijn door een bepaalde bacterie of computervirus. Hieronder worden een aantal veel voorkomende symptomen beschreven.

1.6.1 Regelmatig vastlopen of crashen

Als uw computer helemaal vastloopt en niets meer wil doen, of uw computer gewoonweg crasht (door bijvoorbeeld spontaan opnieuw op te starten) of bepaalde programma's stoppen, of wanneer uw computer opeens een blauw scherm geeft, en als die soort dingen regelmatig voorkomt, dan kan dat wijzen op de aanwezigheid van een computervirus. Een computervirus kan namelijk gemaakt zijn om de computergebruiker lekker te pesten en dit soort ellende te bezorgen.

Het is echter niet per definitie een computervirus. Een nieuw programma dat u juist heeft geïnstalleerd en dat een conflict (met andere software) veroorzaakt, kan hetzelfde effect hebben. Ook het aansluiten van een nieuw toestel op uw computer, bijvoorbeeld een nieuwe scanner of printer, kan hetzelfde effect hebben. Of wanneer er iets in uw computer kapotgaat, zoals de ventilator, kunnen er dergelijke problemen optreden. Tenslotte kan ook een nieuwe versie van een programma dat vroeger altijd goed werkte, ervoor zorgen dat uw computer opeens begint vast te lopen.

1.6.2 Computer werkt heel traag

Als uw computer van de ene dag op de andere heel traag werkt, dan kan dit duiden op een computervirus.

Controleer eerst of het geen eenmalige fout is: sluit uw computer helemaal af en start deze opnieuw op. Als uw computer dan nog steeds zo traag is, dan is er meer aan de hand.

Indien uw computer bijgewerkt is naar een nieuwere versie, bijvoorbeeld van Windows Me naar Windows XP, dan kan uw computer ook opeens trager werken. De oorzaak hiervan is dat het nieuwe besturingssysteem meer geheugen en meer kracht vraagt van uw computer.

---

[1] VYNCKE, P., *Veilig op het internet – De complete gids voor veilig surfen*, Lannoo, Tielt, 2005, 496 pagina's

Controleer of uw harde schijf niet vol is. Het vaste geheugen van uw computer mag niet volledig vol zijn. Indien uw geheugen helemaal vol is, dan zorgt dit ervoor dat uw computer traag gaat werken.

Heeft u pas een nieuw programma geïnstalleerd? Of heeft u een nieuwere versie geïnstalleerd van een bestaand programma? Dit kan er namelijk voor zorgen dat uw computer opeens veel trager werkt, doordat het programma te veel van uw computer vraagt.

Indien hier allemaal geen sprake van is, dan kan dat betekenen dat u een computervirus heeft. Laat in ieder geval een virusscanner uw computer helemaal nakijken.

1.6.3 Niet opstarten

Als uw computer plots niet meer wil opstarten, wil dit niet per definitie zeggen dat uw computer besmet is met een computervirus. Er kunnen nog andere oorzaken zijn. Er kan zelfs gezegd worden dat het in de meeste gevallen niet om een computervirus gaat.

Als het bijvoorbeeld enorm warm is, is het mogelijk dat uw computer gewoon oververhit is. Laat de computer afkoelen en/of probeer de kamertemperatuur te laten dalen.

In de meeste gevallen is er iets stuk aan de computer. De harde schijf kan stuk zijn, uw interne geheugen (RAM-geheugen) kan het begeven hebben, of de ventilator van uw computer. Controleer of uw beeldscherm wel opstaat en of hiermee niets mis is (bijvoorbeeld of de kabel wel goed aangesloten is).

Als uw computer helemaal niet meer wil opstarten, is er niets aan te doen. U zult een specialist moeten raadplegen: iemand uit de familie, een kennis of desnoods iemand uit de winkel waar u de computer heeft gekocht. Zij zullen uw computer wel weer aan de praat krijgen. En als de oorzaak toch een computervirus was, zal men dit achteraf meestal ook kunnen zeggen.

1.6.4 Onverklaarbare activiteit

Als uw computer enorm hard aan het werken is zonder dat hiervoor een verklaring is – u heeft helemaal niets speciaals gevraagd aan uw computer – kan dit wijzen op een computervirus. Uw computer kan traag worden, kan beginnen ratelen (de harde schijf is dan hard aan het werken) en de lichtjes zijn hevig aan het flikkeren; dat zijn de symptomen van onverklaarbare activiteit. Ook een onverklaarbare hoge activiteit van uw internetverbinding kan een aanduiding zijn van een computervirus (vele mensen kunnen via de modem / router / hub de activiteit van hun internetverbinding en/of netwerk zien; wanneer u dit niet kunt zien, kan een plots zeer trage internetverbinding hier ook op wijzen).

De reden van deze hoge activiteit kan verschillende verklaringen hebben. Als het daadwerkelijk om een computervirus gaat, dan is dit computervirus op dit ogenblik volop bezig schade toe te brengen aan uw computer. Het is informatie aan het opzoeken, zich aan het vermenigvuldigen, mogelijk bestanden aan het verwijderen, …

Een andere oorzaak van hoge activiteit van uw computer die u niet kunt verklaren, kan ook betekenen dat een hacker volop bezig is met uw computer. Als een hacker van een afstand toegang heeft kunnen krijgen, kan deze op dit ogenblik uw computer gebruiken om weer bij iemand anders 'in te breken' en zo in uw naam schade toe te brengen aan derden. Het kan ook zijn dat men uw computer gebruikt om massaal ongewenste reclame e-mail te versturen, om een website plat te leggen, …

Nog een andere oorzaak kan zijn dat uw computer zogenaamde spyware bevat. Dit zijn programma's die al uw activiteiten opslaan en dit doorsturen naar derden. Op deze manier kan men niet enkel achter al uw paswoorden komen, maar men kan ook zien wat u allemaal doet op uw pc, men kan uw documenten lezen, …

Uiteraard hoeft een grote onverklaarbare activiteit van uw computer niet altijd onheil te betekenen. Het is best mogelijk dat een programma op uw computer opeens geblokkeerd is en in een zogenaamde 'oneindige lus' is geraakt. Hierdoor geeft het programma tot in het oneindige een bepaalde opdracht steeds opnieuw aan uw computer, waardoor uw computer zeer sterk wordt vertraagd.

Als uw computer een dergelijke onverklaarbare activiteit vertoont, is het beste wat u kunt doen de computer zo snel mogelijk afsluiten. Let erop dat u geen gegevens verliest: sla dus eerst al uw documenten op voor u ze afsluit. Vervolgens start u uw computer opnieuw op.

Wanneer uw computer opnieuw opgestart is en geen onverklaarbare activiteit meer heeft na enkele minuten, dan zal het waarschijnlijk een programma zijn geweest dat was vastgelopen. Wanneer uw computer opnieuw begint met die activiteit, is het het beste om uw internetverbinding uit te schakelen, zodat de hacker niets meer kan doen met uw computer. Vervolgens moet u uw computer scannen met een virusscanner en ook controleren of uw computer (nog) voldoende beveiligd is.

1.6.5 Vreemd computergedrag

Een computer is altijd voorspelbaar. De computer doet onder normale omstandigheden enkel maar wat u vraagt om te doen.

Indien uw computer zich plots vreemd begint te gedragen – bijvoorbeeld wanneer programma's die vroeger altijd werkten, opeens niet meer werken – kan dat wijzen op een computervirus. Er zijn echter nog vele andere dingen die virusschrijvers uitvinden om de aandacht te trekken van hun slachtoffers, zoals:

- Uw computerscherm heeft plots andere kleuren.
- Het scherm begint te flikkeren.
- Uw computer begint opeens vreemde geluiden te maken. Of plots begint iemand u toe te spreken.
- Een document of foto waarvan u zeker bent dat u die gisteren nog had, is opeens weg.
- Een bestand (document, foto, muziek of video) wil niet meer openen. De computer zegt dat het bestand beschadigd is.
- Uw computer vraagt opeens een paswoord terwijl dit vroeger niet zo was. Of als uw computer vroeger wel een paswoord vroeg, wil hij uw (juiste) paswoord niet meer accepteren.
- U krijgt de meest vreemde foutmeldingen op uw computer. Een melding die niets te maken heeft met een handeling die u heeft gedaan op uw computer, maar u bijvoorbeeld opeens feliciteert met uw verjaardag, begint af te tellen of zegt dat u minder moet drinken, … het zijn maar enkele voorbeelden van computervirussen (en hun makers) die graag hun slachtoffer in verwarring brengen.

1.7 Blijf op de hoogte van de nieuwste computervirussen

Het is belangrijk dat u op de hoogte bent van de nieuwste ontwikkelingen op het vlak van computervirussen.

Op het internet zijn er verschillende diensten die bij het verschijnen van een ernstig computervirus of bij andere ernstige veiligheidsproblemen, u onmiddellijk een e-mail sturen. Op die manier bent u niet enkel beschermd door uw virusscanner, maar wordt u ook meteen gewaarschuwd. En een gewaarschuwd man is er twee waard.

Een officiële waarschuwingsdienst in België is het BIPT. U kunt u gratis inschrijven op deze lijst om op die manier op de hoogte gebracht te worden. Inschrijven kan via hun website: http://www.bipt.be.

Een heel interessante website is http://www.virusalert.be. Deze website publiceert heel wat nieuwsberichten over computervirussen en bevat er ook heel wat informatie over. Op deze website kunt u opzoeken welke schade een bepaald computervirus aanricht.

2 Spam

2.1 Wat is spam?

In de internetwereld is spam de verzamelnaam voor ongevraagde en ongewenste e-mailberichten. Andere benamingen voor spam zijn: UCE (Unsolicited Commercial E-mail) en UBE (Unsolicited Bulk E-mail). Ongeveer 30 % van alle e-mails zijn spam en dit percentage neemt dagelijks toe.

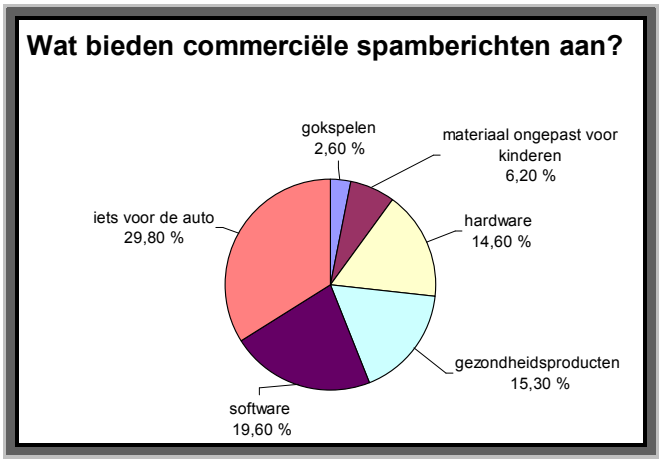
Het verschil tussen spam en 'gewone' e-mails is moeilijk te bepalen want niet elke reclameboodschap of ongevraagde e-mail is spam. Wanneer we over spam spreken, gaat het vooral om een combinatie van onderstaande kenmerken:

- het bericht heeft een commerciële inhoud;
- de afzender heeft het e-mailadres van de geadresseerde willekeurig van internet gehaald;
- het adres van de afzender is vaak vervalst, zodat het niet mogelijk is om te reageren.

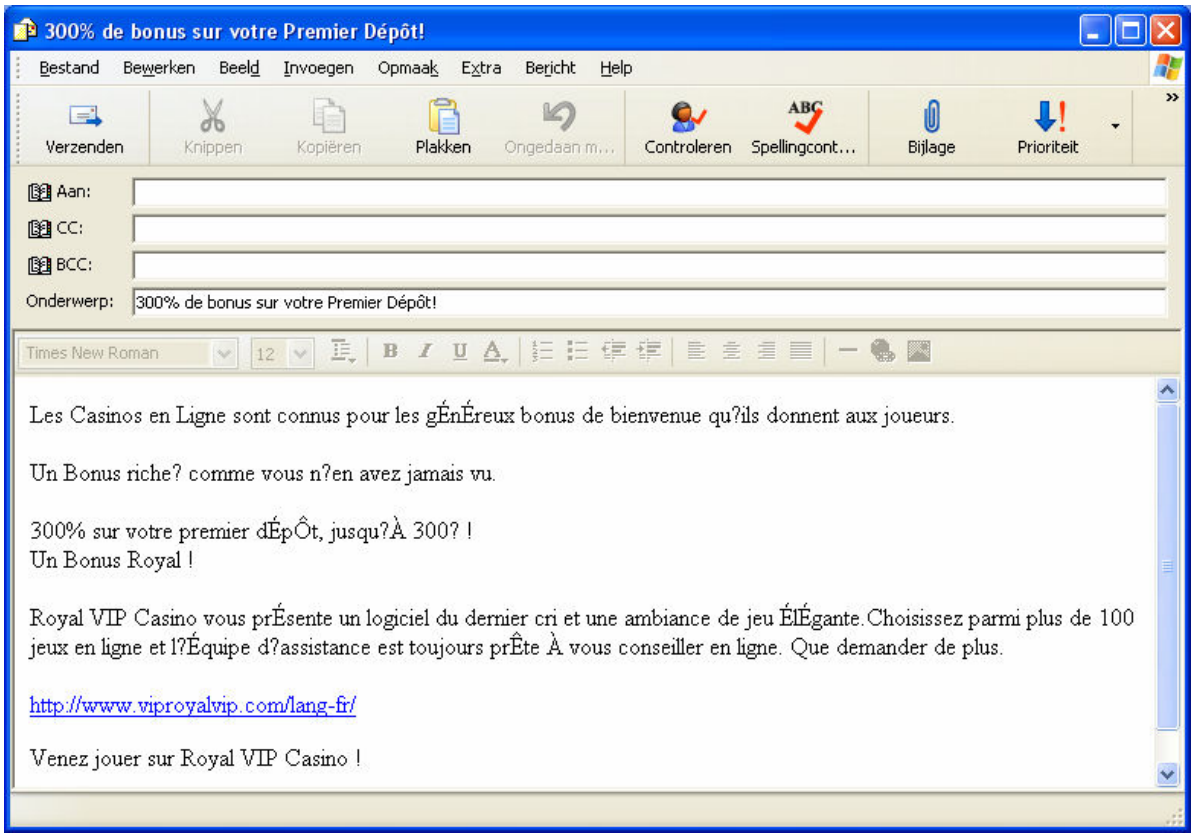
Waarover kan een spambericht zoal gaan?

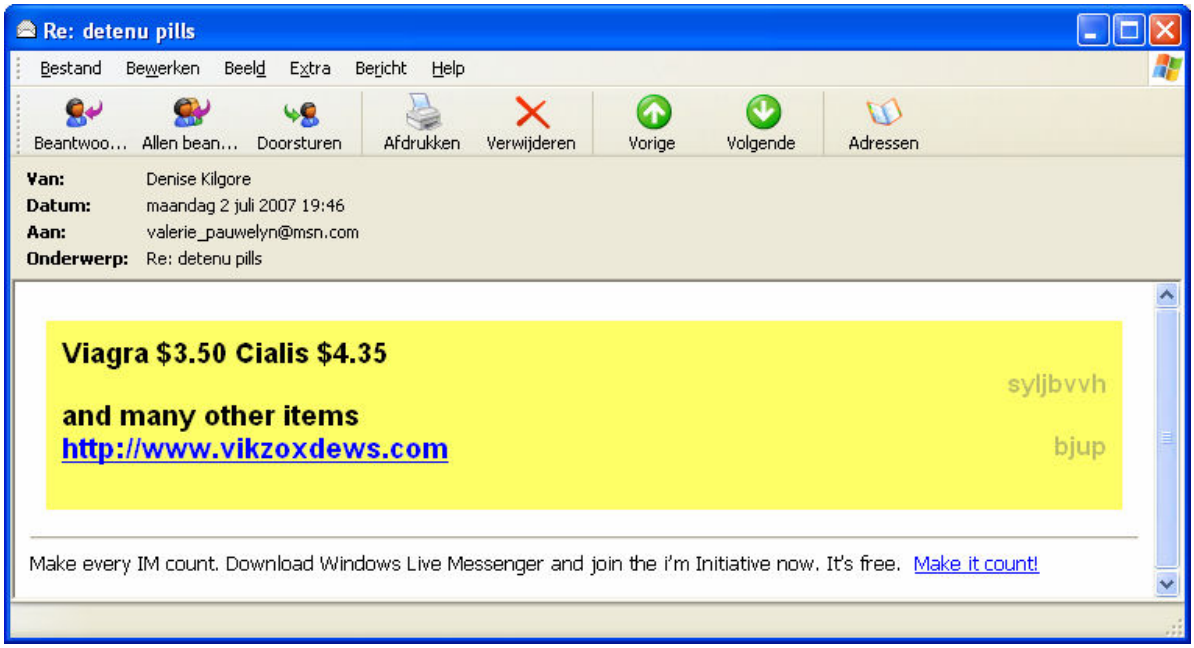
- piramidespelen en andere gokspelen die beweren u snel rijk te maken;
- kettingbrieven;
- advertenties voor pornografische websites of illegale producten;
- seksueel getinte advertenties, medicijnen voor erectiestoornissen, gratis seks, goedkope porno, …;
- verkoop van illegale producten zoals de verkoop van allerlei soorten drugs als XTC, heroïne, cocaïne, …;
- verkoop van (illegale) medicijnen;
- verkoop van goedkopere software;
- …

De spamberichten van commerciële aard, die iets willen verkopen aan de ontvanger van het bericht, kunnen we indelen in zes categorieën:

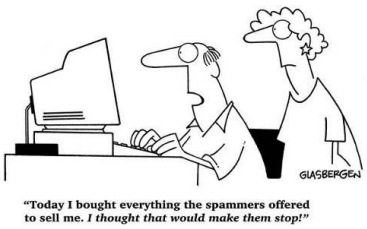


Een paar voorbeelden van spamberichten:





2.2 Wat zijn de gevaren van spam?



"Today I bought everything the spammers offered to sell me. *I thought that would make them stop!*"

Spamberichten zijn niet alleen een van de vervelendste vormen van reclame, maar ze brengen ook gevaren met zich mee.

Uit onderzoek blijkt dat maar liefst 11 % van de internetgebruikers in de val van een spambericht trappen en tot aankoop overgaan, omdat alles er zo aantrekkelijk en voordelig

uitziet. In bijna alle gevallen wordt de koper opgelicht: ofwel wordt het betaalde product niet geleverd ofwel komt de kwaliteit en/of kwantiteit niet overeen met de gegevens uit de spammail (u krijgt bijvoorbeeld een namaakproduct). In de ergste gevallen worden de betalingsgegevens (kredietkaartinformatie) waarmee u eerder het aangekochte goed betaalde (via het principe: eerst betalen, dan pas wordt de bestelling in gang gezet) verder misbruikt om grotere sommen geld van het slachtoffer afhandig te maken.

Spamberichten zijn vaak uit op geld. Soms worden producten of diensten gratis aangeboden, maar 'gratis' is vrijwel altijd onder bepaalde voorwaarden en voor bepaalde tijd. Goedgelovige mensen kunnen zich daarom gemakkelijk laten misleiden en krijgen het na een poosje dan zwaar te verduren.

Bij spamberichten is er ook vaak sprake van inbreuk op de privacy. Wanneer u uw persoonlijke gegevens opgeeft wanneer u iets aankoopt en/of wanneer u zich registreert om een gratis spel te spelen, … kunnen deze misbruikt worden. Uw persoonlijke gegevens kunnen dan worden doorverkocht voor commerciële doeleinden. Als u éénmaal bij een spammer op de lijst staat, is de kans groot dat u niet lang daarna op het lijstje van heel wat spammers staat.

2.3 Hoe kunt u spam proberen te vermijden & hoe gaat u ermee om?

Enkele tips om om te gaan met spam en nog meer spam te vermijden:

- Maak een extra (alternatief) e-mailaccount aan (bijvoorbeeld via Hotmail). Geef dit e-mailadres op aan personen of websites die u niet vertrouwt zoals voor registratie op onbelangrijke websites, het aanvragen van éénmalige informatie, … Op die manier blijft uw privé e-mailadres (dat u doorgeeft aan vrienden, familie, ..) veilig en verkleint u het risico om op dit adres veel spam te krijgen. Wanneer er op uw extra e-mailadres na verloop van tijd te veel rotzooi zoals spam en computervirussen binnenkomen, dan verwijdert u deze of laat u de e-mailaccount verlopen en maakt terug een nieuwe aan. Komt deze tip te laat en ontvangt u momenteel dagelijks tientallen ongevraagde berichten, dan is het beter dat u van e-mailadres verandert. Dit is een drastische maatregel, maar u bent dan wel volledig verlost van de digitale kwelgeesten. Neem er meteen een tweede adres bij om toekomstige spam te vermijden. Al uw vrienden, collega's, familie, … moet u verwittigen van uw nieuw e-mailadres. Ook abonnementen op bepaalde internetdiensten moet u allemaal laten overzetten naar het nieuwe e-mailadres.

- Geef uw e-mailadres en andere persoonlijke gegevens niet zomaar door aan alle websites of personen die erom vragen. Forums, chatrooms en nieuwsgroepen zijn belangrijke bronnen waar spammers hun e-maildressen vandaan halen. Vertrouwt u een bepaalde website niet en is het noodzakelijk om u te registreren, gebruik dan uw alternatief e-mailadres. Zijn uw adresgegevens noodzakelijk en heeft u echt geen vertrouwen in die website, verzin dan iets. Een leugentje voor eigen bestwil…

- Beantwoord nooit spamberichten, het beste is om het bericht gewoon te verwijderen. Door een antwoord te sturen naar de afzender van een spambericht en bijvoorbeeld te vragen om geen berichten meer te sturen, bevestigt u dat uw e-mailadres correct is, waardoor u hoogstwaarschijnlijk nog meer spamberichten zal ontvangen.

- Klik nooit op een hyperlink in een spambericht, zelfs niet op een zogezegde uitschrijflink. Die geven spammers (net zoals het beantwoorden van spamberichten) enkel en alleen maar bevestiging dat uw e-mailadres nog actief is en zo krijgt u hoogstwaarschijnlijk nog meer spamberichten.

- Het is leuk om een zelfgemaakte website op het internet te publiceren, maar let bij deze website ook op welke persoonlijke gegevens u prijsgeeft, want met behulp van speciale zoeksoftware kunnen spammers ook de adressen achterhalen die u op uw website heeft staan. Gebruik hiervoor dus ook best een tweede mailadres.

- Stuur kettingberichten niet door want ook dit type e-mail wordt beschouwd als spam en kan tot ongenoegen leiden bij de ontvanger. Ze worden meestal aanzien als ongewenst en opdringerig.

- Informeer ook uw kinderen, ouders, vrienden, … van de gevaren van spammails. Spijtig genoeg beseffen de meeste mensen onvoldoende dat spam een vorm van oplichting is. Mensen die minder of niets afweten van internetgevaren zijn immers voor spammers een perfecte doelgroep.

Als u de voorgaande tips volgt, dan herleidt u de kans op spam tot een minimum. Zijn de vorige tips tevergeefs geweest (wat ik sterk betwijfel) dan zijn er nog andere mogelijkheden om hard op te treden tegen spam:

- U kunt in pricipe een klacht neerleggen tegen een spammer. Hiermee zult u meestal enkel de kleine spammers aanpakken. De 'grote spammers' zullen valse afzenders gebruiken, hun IP-adres verbergen, … Enkel de kleine kunnen worden opgespoord en gestopt. Wilt u een klacht indienen dan moet u het originele bericht doorsturen naar de Commissie voor bescherming van de persoonlijke levenssfeer. Het e-mailadres is spam@privacy.fgov.be. Zij zullen het dan voor u verder afhandelen, ook als het bericht uit het buitenland komt. Dit is één van de mogelijke meldpunten. Er bestaan nog andere maar dit is één van de eenvoudigste en betrouwbaarste manieren om spam aan te klagen.

- Om spam in te perken, kunt u gebruik maken van een filter. Spamfilters zijn gebaseerd op regels (bijvoorbeeld: in de e-mail komt het woord spam, drugs, sex, … voor). Indien een e-mail aan één van die regels voldoet, kan de filter bijvoorbeeld de e-mail definitief verwijderen, onmiddellijk naar de prullenbak verplaatsen, … Via filters kunt u ook afzenders blokkeren zodat u bijvoorbeeld van bepaalde personen geen e-mails meer hoeft te lezen. De meeste e-mailprogramma's (bijvoorbeeld Outlook Express) bieden zo'n service aan. Belangrijk hierbij te vermelden is dat dergelijke filters zelden gebruikt worden omdat spammers bijna nooit met hetzelfde e-mailadres spammen (tenzij bijvoorbeeld een kettingmail van een vriend/vriendin). Ook spammers zijn zich bewust van de regels die een gebruiker kan toevoegen en proberen deze op alle mogelijke manieren te omzeilen. U kunt zich bij filters afvragen of ze wel de moeite waard zijn om te gebruiken als middel tegen spammers.

- Wie niet van ongewenste reclame houdt, kan dat aangeven door zich in te schrijven op de elektronische Robinson-lijst. Hierdoor weten de aangesloten bedrijven dat ze u geen mails hoeven te sturen. Helaas heeft dit maar een beperkt effect: echte massamailers houden er geen rekening mee, maar alle beetjes helpen natuurlijk. Wilt u zich op deze

lijst inschrijven dan kunt u dit doen door te surfen naar http://www.robinsonlist.be waar u alle Nederlandstalige uitleg vindt.

3 Hackers

Uw huis beschermen tegen inbrekers doet u door een stevig slot op uw deuren te plaatsen, uw ramen en deuren te sluiten als u weg bent en, indien u waardevolle dingen in huis heeft, een alarmsysteem te plaatsen, Wel, hetzelfde zou u moeten doen voor uw computer. Het is namelijk zo dat er minstens evenveel inbrekers zijn, die in uw computer willen inbreken, als er inbrekers zijn die in huizen inbreken. We kunnen dus een hacker vergelijken met een inbreker.

Een gewone inbreker kan niet rondlopen met een levensecht masker van een andere (bestaande) persoon. Dit is spijtig genoeg wel mogelijk op het internet. Een hacker doet zich namelijk voor als iemand anders. Een juridisch onderzoek kan dus ook leiden naar de verkeerde persoon, omdat de hacker een 'masker' van iemand anders droeg, en ook u kunt hiervan het slachtoffer worden. U hiertegen beveiligen is dus geen overbodige luxe.

3.1 De geschiedenis van de hackers[1]

We beginnen met de geschiedenis van het hacken in 1971. Eigenlijk kunnen we het nog niet echt hacken noemen. Een zekere John Drapper ontdekt dat als hij een toestel, later de blue box genoemd, in de buurt van een betaaltelefoon plaatst, dit hem toelaat gratis te telefoneren. Zijn toestel produceert namelijk een geluid met exact dezelfde frequentie als waarmee wordt doorgegeven dat de gebruiker geld in het toestel steekt.

Het echte hacken start pas in 1981: toen heeft een zekere Ian Murphy ingebroken bij AT&T in Amerika en heeft daar de systeemklok gewijzigd, waardoor gebruikers rekeningen kregen voor telefoontjes die ze 's nachts pleegden terwijl ze 's middags telefoneerden en omgekeerd.

Dan blijft het een tijdje betrekkelijk rustig, totdat in 1984 Bill Landreth erin slaagt om in te breken bij de NASA. Intussen worden er steeds meer groepjes van hackers gevormd, maar zij slagen er niet in om unieke inbraken te plegen.

In 1986 slaagt een groepje Duitse hackers erin om informatie te stelen van een geheim rapport in verband met de Chernobyl-crisis. In hetzelfde jaar slaagt een tot nu toe onbekende groep hackers erin om voor tienduizend dollar schade te berokken bij de Stanford University.

Vanaf 1987 worden de NASA en andere grote instanties steeds geregelder het slachtoffer van hackers. Vervolgens blijft het weer rustig. Er worden wel systemen gekraakt, maar nooit iets nieuws. Men heeft het steeds op dezelfde systemen gemunt: het telefoonsysteem, de NASA en enkele andere grote doelwitten.

In 1991 wordt voor het eerst een lijst met creditcardnummers ontvreemd en misbruikt.

In 1994 wordt Richard Pryce, een zestienjarige, veroordeeld wegens het inbreken in honderd computersystemen, waaronder dat van de Griffiths Air Force basis, de NASA en het Koreaanse Atoomonderzoekscentrum. In hetzelfde jaar slaagt Vladimir Levin, een Russi-

[1] VYNCKE, P., *Veilig op het internet – De complete gids voor veilig surfen*, Lannoo, Tielt, 2005, 496 pagina's

sche hacker, erin om de eerste digitale bankoverval te plegen, hij maakte tien miljoen dollar buit van Citybank.

In 1995 slaagt Corey Lindsly, leider van de hackersgroep 'Phonemasters', erin om de telefoonsystemen van AT&T, British Telecom, GTE, MCI WorldCom, Sprint en Southwestern Bell binnen te dringen. Bovendien slaagt de groep erin om de systemen van enkele overheidsinstanties binnen te dringen, alsook in enkele databanken met creditcardnummers. Bovendien krijgen ze toegang tot de elektriciteitssystemen, luchtverkeersleidingen en geraken ze aan geheime nummers van het Witte Huis.

In hetzelfde jaar wordt Chris Lamprecht als eerste ooit door de rechtbank verboden om nog op het internet te surfen.

Verder wordt in 1995 door de Franse student Damien Doligez de eerste 40-bitscodeermethode gekraakt. Ook wordt er in 1995 voor het eerst iemand naar de gevangenis gestuurd voor een computermisdrijf: Christopher Pile zal voor achttien maanden in de cel zitten wegens het schrijven van een computervirus.

In 1996 wordt bekendgemaakt dat er in 1995 maar liefst tweehonderdvijftigduizend keer een poging werd gedaan om in te breken in de bestanden van het US Defense Department. 65 % van deze aanvallen waren volgens het rapport ook succesvol.

In 1996 slagen hackers in Amerika erin om de boodschap op het automatische antwoordapparaat van de hulpdiensten 911 in New York te wijzigen in 'officers are too busy eating doughnuts and drinking coffee to answer the phones' (de agenten zijn te druk bezig met het eten van donuts en het drinken van koffie om de telefoon op te nemen).

In 1997 wordt door de zesendertigjarige Carlos Felipe Salgado voor het eerst een sniffer-programma gebruikt. Dit programma werd op een server geplaatst en scande automatisch alle e-mails die voorbijkwamen op creditcardgegevens. Op deze manier zou hij honderdduizend creditcardgegevens hebben kunnen verzamelen. In hetzelfde jaar wordt voor het eerst een grote website tijdelijk onbereikbaar gemaakt: het slachtoffer is Yahoo.com.

In 1998 worden de broers Hao Jinglong en Hao Jingwen in China voor het eerst tot de doodstraf veroordeeld wegens hacken. Ze braken bij een bank in en stalen zevenhonderdtwintigduizend yuan (zevenentachtigduizend dollar). Uiteindelijk wordt enkel Hao Jingwen ter dood veroordeeld; zijn broer krijgt een lichtere straf omdat hij meewerkte aan het onderzoek.

In april 1998 wordt voor het eerst de mailbom gebruikt. Iemand uit Alabama verstuurt veertienduizend e-mailberichten naar het NASA-netwerk. In juli wordt Back Orifice gepubliceerd op het internet. Deze Trojan maakt het mogelijk om de controle over de computer van het slachtoffer volledig over te nemen. In september slagen hackers erin om de website van The New York Times te wijzigen in 'Hacking for Girls'.

In 1999 begint Napster bekendheid te verkrijgen voor het uitwisselen van bestanden, waarop auteursrechten berusten, zonder dat men ervoor moet betalen. In juli 2001 zal deze dienst uiteindelijk worden opgedoekt. Intussen hebben ze vijfentachtig miljoen geregistreerde gebruikers gehad die samen drie miljard liedjes downloadden per maand. In hetzelfde jaar sluit Microsoft zijn dienst Hotmail voor een tweetal uren, omdat er een ernstig lek is waardoor hackers zonder gebruik van wachtwoorden toegang krijgen tot alle accounts. In dit jaar worden ook heel wat andere websites platgelegd en gewijzigd. ABC News, Drude Report, Nasdaq, American Stocket Exchange en de website van het Witte Huis moeten eraan geloven. In november van 1999 vindt de vijftienjarige Noor Jon Johansen een manier om de code te kraken waarmee alle dvd's op dat moment beveiligd zijn.

Op 7 februari 2000 wordt voor het eerst echt gebruik gemaakt van de zogenaamde DDoS-aanvallen (distributed denial-of-service). Door het overvloedig sturen van informatie naar

een bepaalde website kan men deze website onbereikbaar maken voor het publiek. Als eerste moet Yahoo eraan geloven, twee dagen later worden ook eBay, Amazon, Buy.com, ZDNet, CNN, E*Trade en MSN het slachtoffer.

In oktober 2000 wordt de server AntiOn-line, die volgens de eigenaars 'onkraakbaar' werd genoemd, na maar liefst negen miljoen hackpogingen toch gekraakt door een Australiër. In december worden vijfenvijftigduizend creditcardnummers gestolen van Creditcards.com, vijfentwintigduizend daarvan worden gewoon op het internet gepubliceerd.

Op 1 februari 2001 slagen hackers erin informatie te krijgen over heel wat belangrijke personen. De informatie bevatte creditcardnummers, nummers van mobiele telefoons, thuisadressen, paspoortnummers, enz. over Bill Gates, Yasser Arafat, Kofi Annan, Madeline Albright en de Israëlische eerste minister Shimon Peres. Op 12 februari maakt de FBI bekend dat er bij een veertigtal internetwinkels ingebroken is en er in totaal 1 miljoen creditcardnummers gestolen werden. In juli slaagt de hackersgroep 'World of Hell' erin om zeshonderdnegenenzeventig websites te wijzigen in slechts één minuut tijd. In augustus wordt van Riggs Bank de Visa-databank van al hun klanten gestolen.

Op 21 oktober 2002 wordt er een ernstige DDoS-aanval uitgevoerd op de dertien rootservers van het internet. Als ze deze dertien 'down' krijgen, ligt het volledige internet plat. Het is niet zover gekomen, maar enkele servers zijn toch down gegaan; het internet heeft er echter vrijwel niets van ondervonden.

In februari 2003 slaagt een hacker erin om acht miljoen creditcardnummers te stelen van Visa, MasterCard en American Express. Op 29 april wordt de hacker gearresteerd die inbrak in vele websites, waaronder die van McDonalds, Symantec, SecurityFocus en SANS Institute.

3.2 Hackers, crackers en script kiddies

Mensen die inbreken in computers kunnen we indelen in drie grote groepen: hackers, crackers en script kiddies.

Door de (korte) geschiedenis heen, wordt de term hacker als verzamelnaam gebruikt voor zowel de echte hackers, de script kiddies als de crackers (ook al zijn er verschillen tussen deze groepen). In de rest van dit eindwerk zal de verzamelnaam hacker gebruikt worden, dit om de duidelijkheid en de samenhang van dit eindwerk te stimuleren. Toch worden de drie grote groepen even verduidelijkt.

3.2.1 Hackers

Een hacker, ook wel computerkraker genaamd, is iemand die zonder kwade bedoelingen inbreekt in een computersysteem. Hackers willen crackers voor zijn door te zoeken naar veiligheidslekken en op die manier systemen binnen te komen. Eenmaal ze toegang tot het systeem hebben bemachtigd, doen ze niets verkeerds. Integendeel, ze melden de eigenaar(s) van de server of de programmeur(s) van het softwarepakket dat er een lek is. Hierdoor kunnen de eigenaars hun product verbeteren en voorkomen dat de crackers het systeem van hun klanten binnendringen, bv. om de zwakke plekken daarvan aan te tonen.

In tegenstelling tot wat de meeste mensen denken, zal een hacker niets vernietigen maar juist proberen iets te verbeteren.

3.2.2 Script kiddies

Script kiddies zijn een grotere groep dan hackers en crackers. Script kiddies zijn personen die nog aan het 'leren' en oefenen zijn hoe ze in feite moeten inbreken in een computer. Hiervoor maakt een script kiddie gebruik van allerlei exploits. Exploits zijn programma's die geschreven worden door crackers en die het makkelijk maken om dankzij een veiligheidslek iets te kunnen doen wat normaal niet de bedoeling is zoals bijvoorbeeld bestanden wissen op de computer van iemand anders, …

De script kiddie gebruikt deze exploits om zich te amuseren en voor de kick. Ze zijn het meest bedreigend voor de gewone computergebruiker want vaak willen ze hun kennis testen bij computers van mensen die ze kennen.

3.2.3 Crackers

Crackers zijn de gevaarlijkste groep mensen die inbreken in computers, want ze gaan verder dan een script kiddie. Het zijn criminele computerinbrekers. Crackers zijn mensen die vroeger script kiddie zijn geweest, maar ondertussen al heel wat hebben bijgeleerd. Een cracker zoekt zelf veiligheidslekken en schrijft er zelf exploits voor.

Crackers hebben de bedoeling om dingen stuk te maken en zo te laten zien wat ze kunnen. Er zijn heel wat crackers die geld willen slaan uit hun kennis door bijvoorbeeld bij banken of andere instellingen in te breken en dan een grote geldsom op een anonieme rekening over te schrijven en te verbruiken.

3.3 De verschillende soorten hackers

Wat is de reden dat hackers het op een bepaalde computer gemunt hebben? Wel, er zijn een vijftal soorten hackers die elk hun eigen motief hebben:

- De minst gevaarlijke hackers zijn diegenen die enkel willen achterhalen welk systeem er op een bepaalde computer gebruikt wordt en welke gegevens er op de harde schijf te vinden zijn. Indien de hacker geïnteresseerd is, kan hij ook enkele gegevens kopiëren. Vaak gaat het hier om mensen die nog maar aan het leren hacken zijn.

- Er zijn ook hackers die een bepaald doel voor ogen hebben: zorgen dat het de computergebruiker geld en tijd zal kosten om de aangerichte schade van de hacker te herstellen. Deze hackers kunnen we vandalen noemen. Wat richt zo'n type vandaal dikwijls aan?
    - het systeem laten vastlopen;
    - persoonlijke gegevens bekijken;
    - uw toetsenbord (of enkele letters ervan) buiten werking stellen;
    - bestanden wijzigen;
    - bestanden verwijderen;
    - alle gegevens wissen;
    - de harde schijf formatteren;
    - uw internetverbinding gebruiken om bijvoorbeeld breedbandrovende en/of illegale zaken (programma's, films, …) te downloaden
    - …

- Een ander soort hackers zijn high-profile hackers. Dit zijn hackers die zich vooral interesseren in het kraken van 'beroemde' systemen zoals die van het Witte Huis, Microsoft, Google, … Een high-profile hacker hackt meestal om de roem en status die hij/zij krijgt in het wereldje van de hackers als een dergelijke computerinbraak lukt.

- Daarnaast zijn er ook 'huurhackers'. Sommige bedrijven huren ook hackers in om de systemen van hun concurrenten of zelfs hun eigen systeem te hacken. Als een bedrijf een hacker inhuurt om een systeem van een concurrent aan te vallen, dan is dit in de meeste gevallen om gegevens te stelen, gegevens te vernietigen of om gegevens te wijzigen zodat ze zelf voordeel kunnen halen uit het feit dat het slachtoffer deze data kwijt is. Sommige bedrijven huren zelf een hacker in om te proberen hun systeem te hacken. Als de hackers een veiligheidslek vinden, dan kan uw producent proberen het probleem weg te werken. Bij de ontwikkeling van het besturingssysteem Windows Vista werden er bijvoorbeeld enkele hackers ingehuurd om op zoek te gaan naar veiligheids-lekken die men dan later verbeterde.

- Een andere veel voorkomende soort hackers zijn 'leners' die een computer gebruiken voor verscheidene doeleinden die niet altijd even legaal zijn. Ze gebruiken namelijk uw processortijd of harde schijfruimte om iets te bereiken. Bovendien kunnen ze uw internetverbinding gebruiken en dus ook uw down- en uploadvolume. Ze kunnen ook uw identiteit gebruiken, als masker op het internet. Alles wat ze dan (verkeerd) doen, zal op u verhaald worden.

3.4 Hoe uw gegevens beveiligen tegen hackers?

3.4.1 Het wachtwoord

Een wachtwoord is een 'formule', die gebruikt wordt om te controleren of iemand die zich aanmeldt toegang mag worden verleend. Zo kunt u een e-mailaccount, een computer, een gebruikersaccount, … beveiligen met een wachtwoord.

Het is belangrijk dat u een wachtwoord kiest dat u zelf gemakkelijk kunt onthouden en dat niet al te logisch is (niet uw geboortedatum, de naam van uw kind, van uw vriend, …). Zorg ervoor dat een hacker uw wachtwoord niet zomaar kan raden.

Een wachtwoord, dat bestaat uit één woord, is niet aan te raden. Als het een woord is, dat voorkomt in het woordenboek, heeft een hacker het zo gevonden. Er zijn namelijk kant-en-klare programmaatjes beschikbaar die heel het woordenboek afgaan en alles proberen als paswoord. Een dergelijke aanval wordt dan ook een woordenboekaanval ofwel dictionary attack genoemd. Een dergelijk woordenboek bevat veel gebruikte paswoorden. Dit is een zeer uitgebreide lijst van gewone woorden uit het woordenboek, maar met ook veel voorkomende namen, plaatsnamen, voetbalteams, enz. En zo bestaan er enorm veel woordenboeken. Er bestaan ook speciale woordenboeken voor een aanval in bepaalde landen. Neem nu voor België of Nederland. In een dergelijk woordenboek staan dan heel wat woorden uit de Van Dale, maar ook heel wat namen van steden en streken in België en Nederland, de namen van voetbalploegen en van beroemde plaatselijke mensen, en ook heel wat namen die typisch zijn voor onze streken, bijvoorbeeld Janssens, Peeters, Jef, Jan, Filip, ... Zulke programma's proberen duizende paswoorden per seconde en verlenen dus toegang tot heel wat computers met een (te) simpel paswoord in enkele seconden.

Uit Engels onderzoek bleek dat 47 % van de ondervraagden zijn of haar eigen naam of koosnaampje als wachtwoord gebruikt. 32 % gebruikt de naam van zijn of haar favoriete voetbalteam of van hun idool. Met andere woorden, bij 79 % van de ondervraagde mensen raakt u zo binnen als u een goed woordenboek heeft voor een woordenboekaanval!

Het ideale paswoord bestaat uit een combinatie van kleine letters, hoofdletters, cijfers en een 'vreemd teken' (, - / [! …) zoals bijvoorbeeld 'z2*akF,R5'. Makkelijker gezegd dan gedaan, want onthoud dit wachtwoord maar eens naast alle andere wachtwoorden die u al heeft. Toch zijn er verschillende manieren om een moeilijk raadbaar, maar toch makkelijk te onthouden wachtwoord te maken. Zo kunt u er bijvoorbeeld voor opteren om in al uw

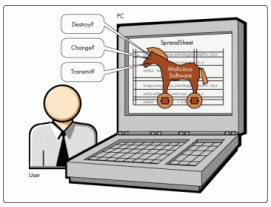
wachtwoorden de E-letter in hoofdletter te plaatsen en op het einde van het wachtwoord het aantal cijfers van het wachtwoord te plaatsen. Een andere tip is om als wachtwoord een zin te gebruiken in plaats van één woord, we noemen dit wachtzinnen. Wachtzinnen kunnen lang en complex zijn en toch gemakkelijk te onthouden. Een voorbeeld van een wachtzin is: 'Roze, blauw en wit zijn mijn lievelingskleuren!'.

Samengevat: zorg voor een moeilijk wachtwoord, maar makkelijk te onthouden.

"Sorry voor de geur. Al mijn wachtwoorden staan getatoeëerd tussen mijn tenen."

Daarnaast is het ook niet veilig om hetzelfde wachtwoord te gebruiken voor alle accounts, programma's, computers, … waarvoor u een wachtwoord nodig heeft. Men kan namelijk ook 'gemakkelijk' aan uw paswoord geraken door gewoon over uw schouders mee te kijken wanneer u uw paswoord intikt. Zogenaamde keyloggers, die alle toetsaanslagen opslaan, kunnen vervolgens uw wachtwoord hieruit filteren. Als men dat ene paswoord heeft gevonden, kan men onmiddellijk alles in uw plaats doen, en zo maakt u het de hackers wel heel erg gemakkelijk. Daarom is het beter om voor elke dienst, elk programma en elke plaats waar u een wachtwoord nodig heeft, een ander te gebruiken. Er bestaan nu zelfs al gratis programmaatjes zoals MyKeyRing waarin u al uw loginnamen en wachtwoorden kunt bewaren. Met één wachtwoord dat het programma beveiligt, heeft u toegang tot al uw wachtwoorden.

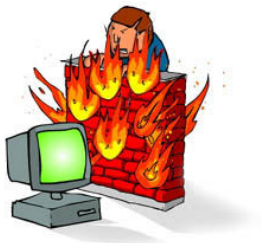
3.4.2 Het Trojaanse paard



Hackers maken handig gebruik van Trojaanse paarden. Dankzij dit programma kan een hacker snel en gemakkelijk de controle over uw computer overnemen: de 'deuren' van uw computer worden als het ware wagenwijd opengezet. Zorg dus voor een goed antivirusprogramma dat ook dit soort computervirussen kan opsporen en verwijderen. Ook de firewall kan Trojaanse paarden tegenhouden.

3.4.3 De firewall

Voor elk probleem bestaat er een oplossing en dit is niet anders bij hackersaanvallen; de oplossing is een firewall.



Een firewall is voor thuisgebruikers een softwarebescherming (in bedrijven wordt vaak ook gebruik gemaakt van een hardware firewall) voor computers die in verbinding staan met het internet: het staat tussen uw computer en de buitenwereld (het internet). Een firewall bemoeit zich niet met wat er gebeurt op uw pc zelf en bemoeit zich alleen met de dingen die tussen uw computer en de buitenwereld gebeuren. De firewall bekijkt namelijk ieder pakketje informatie dat tussen uw computer en de buitenwereld (het internet) uitgewisseld wordt. Een firewall sluit alle 'poorten' van uw pc en opent alleen maar de poorten waarvoor u toestemming geeft.. U moet u een dergelijke poort niet voorstellen als iets echt 'zichtbaars'. Het is meer een uniek nummer op uw computer dat het systeem vrijgeeft om te kunnen praten met de buitenwereld. Voor surfen wordt bijvoorbeeld meestal poort tachtig gebruikt, voor e-mail meestal poort vijfentwintig.

De firewall bekijkt alle pakketjes één voor één: van wie komt de informatie en waar gaat die naartoe? Bovendien zal hij bepaalde afzenders blokkeren. De firewall heeft op het gebied van het controleren van informatiepakketjes een vetorecht. Als het hem niet aanstaat, wordt het pakketje niet doorgelaten en wordt het onverbiddelijk 'vernietigd'.

In de praktijk is het zo dat u bepaalde programma's op uw computer toelating geeft om te communiceren met het internet. De programma's die géén toelating hebben gekregen, kunnen dan ook niet communiceren met de buitenwereld (via het internet).

Een firewall vormt onder andere een barricade voor Trojaanse paarden (programma's) die mogelijks op uw computer actief zijn (normaal gezien heeft u van hun aanwezigheid zelfs geen weet). De firewall zal geen toelating geven aan deze programma's om te communiceren met de buitenwereld met als gevolg dat de werking van de Trojaanse paarden tegengehouden wordt. Het Trojaanse paard kan uw computer niet meer 'wagenwijd openzetten' want het kan immers niet meer met het internet communiceren. Dit is echter alleen van toepassing wanneer uw firewall ook uitgaande verbindingen kan blokkeren (de firewall van Windows XP doet dit niet). Meestal hebben de gratis firewall's enkel de mogelijkheid om inkomende pakketjes te controleren en niet de uitgaande.

Er zijn heel wat programma's met veiligheidslekken. Hackers zoeken deze veiligheidslekken en maken er gretig gebruik van om uw computer binnen te geraken. Maar met een goede firewall is dit dus ook geen probleem meer, omdat hij alles sluit en tegenhoudt.

Een firewall is een goede bestrijding, maar er zijn natuurlijk ook nadelen; er zijn er meer bepaald drie:

- Een firewall vertraagt de internetverbinding omdat hij alles wil controleren of het wel veilig is.
- Een firewall vertraagt de computer want het controleren van het internetverkeer slorpt ook gebruiksgeheugen en processorcapaciteit op en dit heeft een tragere computer tot gevolg.
- Een derde nadeel is dat u zich soms te veilig voelt met een firewall en dat u niet meer alert bent. U bent nooit 100 % veilig, want ook firewalls kunnen bijvoorbeeld veiligheidslekken hebben.

Er zijn heel wat firewalls op de markt en ook hier heeft u betalende en gratis versies zoals:

- ZoneAlarm (http://www.zonealarm.com) ⇨ gratis firewall;
- McAfee firewall (http://www.mcafee.com);
- Norton personal firewall (www.norton.com);
- …

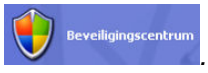
Sinds de komst van Service Pack 2 voor Windows XP bevat het besturingssysteem ook zelf een firewall namelijk de *Windows Firewall*. U hoeft dus niet per se een firewall te downloaden want de ingebouwde firewall biedt 'voldoende' bescherming. Is er reeds een andere firewall actief, schakel dan de Windows Firewall uit. Net zoals bij antivirusprogramma's is het ook bij firewall's niet aangeraden om twee of meerdere firewall's te gebruiken (er zouden conflicten kunnen ontstaan).

De Windows Firewall kunt u al dan niet uitschakelen via de volgende stappen:

1 Ga naar *Start* 

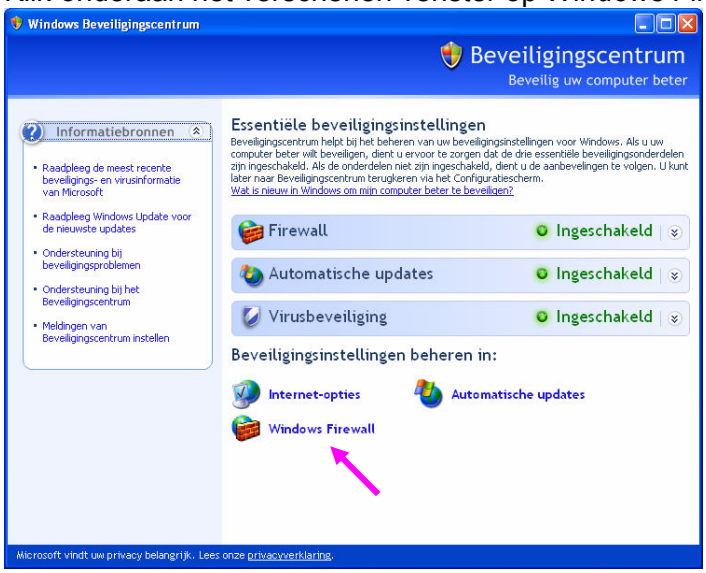
, *Configuratiescherm* 

.

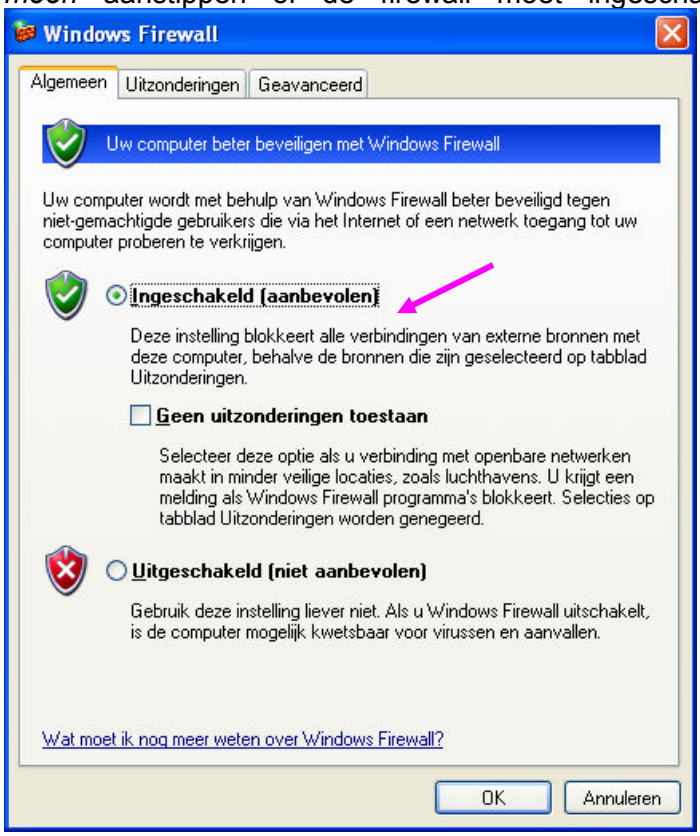
2 Kies voor de categorie *Beveiligingscentrum* 

.

3 Klik onderaan het verschenen venster op *Windows Firewall.*



4 In het volgende venster kunt u de *Windows Firewall* configureren. In het tabblad *Algemeen* aanstippen of de firewall moet ingeschakeld of uitgeschakeld worden.



4 Spyware

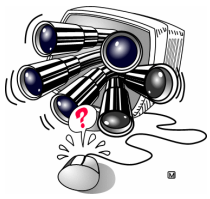
4.1 Wat is spyware?

Spyware is software (een programma). Een programma dat u in feite 'bespioneert' door informatie te verzamelen over wat u op uw computer doet en die informatie doorstuurt naar de maker(s) van die spyware. Zo registreert spyware welke websites u bezoekt, hoeveel uren u surft, hoeveel e-mails u verstuurt en ontvangt, welke programma's u zoal gebruikt, …

Spyware installeert u buiten uw wil om en meestal weet u niet eens dat er spyware op uw computer actief is. Spyware wordt mee geïnstalleerd wanneer u een of ander computerprogramma installeert dat u vaak gratis kunt downloaden van het internet (freeware). Wanneer u bijvoorbeeld het PnP-programma Bearshare (waar u onder andere illegaal liedjes kunt downloaden) downloadt, downloadt u ook automatisch spyware (toch bij enkele verschillende versies van dit programma).

Wat doen die makers van spyware nu precies met uw gegevens en met die van wellicht duizenden anderen? Wel, via deze persoonlijke informatie kunnen ze uw voorkeuren te weten komen en op die manier reclamebanners aanpassen aan uw interesses. U ziet die reclamebanners meestal wanneer u een bepaald programma opent (het programma waarmee samen de spyware werd geïnstalleerd) en/of wanneer u bepaalde websites bezoekt. Soms kunnen de spywarebedrijven ook uw e-mailadres achterhalen en u zo overladen met e-mails die reclame bevatten voor producten die aanleunen bij uw interesses. Deze e-mails zijn ongewild en dan spreken we natuurlijk van spam.

4.2 Wat zijn de nadelen van spyware?



Spyware is een inbreuk op uw privacy (aangepaste reclamebanners en/of e-mails met reclame voor één of ander product). Daarnaast kan spyware ook uw internetverbinding en zelfs uw computersysteem (flink) vertragen waardoor de computer kan vastlopen. Volgens een onderzoek van Microsoft blijkt dat de oorzaak van de gecrashte computers in 50 % van de gevallen veroorzaakt werd door spyware.

4.3 Hoe kunt u spyware voorkomen?

Het is moeilijk om spyware te voorkomen want, zoals eerder al gezegd, heeft u het meestal niet door wanneer spyware meegeïnstalleerd wordt bij een of ander programma. Sommige pagina's (om zichzelf te beschermen) vermelden wel dat er een mogelijkheid bestaat dat samen met hun programma ook spyware wordt geïnstalleerd. Die vermelding staat dan vaak in kleine lettertjes in de gebruikersovereenkomst die u al dan niet accepteert (niet accepteren betekent geen installatie van het programma). Als u een dergelijke vermelding ziet, moet u zich afvragen of u liever op zoek gaat naar een ander programma of als u liever heeft dat uw persoonlijke gegevens doorgestuurd worden.

Het is ook belangrijk dat u een firewall gebruikt die uitgaande verbindingen controleert. Op die manier kunt u alle uitgaande verkeer blokkeren en/of controleren. Geef niet alle programma's toegang om te communiceren met het internet. Let dus goed op welke programma's u niet laat blokkeren door uw firewall.

Om spyware vroegtijdig de rug toe te keren is het belangrijk om toch regelmatig uw volledige computer te laten scannen op spyware. U doet dit door gebruik te maken van een anti-

spywareprogramma. Hieronder vindt u verder meer informatie. Als u een fanatieke internetgebruiker bent, is een wekelijkse antispywarescan geen overbodige luxe.

4.4 Hoe kunt u spyware verwijderen?

Meestal heeft u er geen weet van dat uw computer spyware bevat. De ideale oplossing hiervoor is om een antispywareprogramma te gebruiken dat detecteert of u spyware op uw computer heeft. Een goed antispywareprogramma kan ook de spyware van uw computer verwijderen want door het moederprogramma (waarmee de spyware mee werd geïnstalleerd) handmatig te verwijderen, wordt de spyware zelf niet gedesinstalleerd.

Een lijstje van enkele antispywareprogramma's die doeltreffend blijken te zijn; sommige zijn gratis, andere zijn betalend. Natuurlijk is dit maar een greep uit het aanbod:

- Hitman Pro (http://www.hitmanpro.nl)
- Windows Defender (http://www.microsoft.com/athome/security/spyware/software) Dit programma zit standaard in Windows Vista maar voor Windows XP- en Windows 2003 Server- gebruikers kunt u het antispyware programma op dit internetadres downloaden)
- Ad-aware (http://www.lavasoft.com)
- Spybot – Search & Destroy (http://www.safer-networking.org)
- Spyware Doctor (http://www.pctools.com).
- CounterSpy (http://www.sunbelt-software.com/Business/Counterspy-Enterprise)

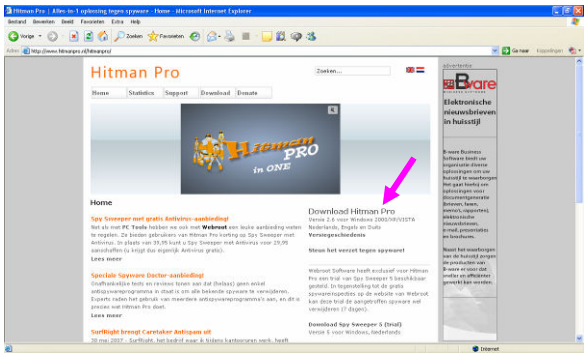
4.4.1 Het antispywareprogramma Hitman Pro downloaden en installeren voor gebruik

Een van de betere Nederlandstalige antispywareprogramma's is *Spyware Doctor;* het heeft zelfs al een aantal prijzen/titels in de wacht kunnen slepen. Op de website van http://www.pctools.com kunt u een gratis versie van het antispywareprogramma downloaden waarmee de spyware gedetecteerd en geblokkeerd wordt. Om van alle voordelen van het programma te kunnen genieten, moet u zich de betalende versie aanschaffen en die versie heeft de meerwaarde dat ze de spyware verwijdert.

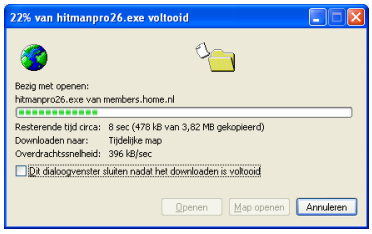
Ook het gratis en Nederlandstalige programma *Hitman Pro* wordt door gebruikers hoog in het vaandel gedragen. Wanneer u het programma installeert, worden er enkele verschillende antispywareprogramma's op uw computer geïnstalleerd zodat u uw veiligheid niet alleen toevertrouwt aan één antispywareprogramma. Hitman Pro zorgt ervoor dat de spyware gedetecteerd en automatisch verwijderd wordt.

Wilt u *Hitman Pro* installeren, volg dan onderstaande werkwijze.

	Open uw internetbrowser (bijvoorbeeld *Internet Explorer*) en surf naar de website http://www.hitmanpro.nl



Klik op de hyperlink *Download Hitman Pro*.



U krijgt een beveiligingswaarschuwing, klik op de knop *Uitvoeren* of *Opslaan.*
Kiest u voor de optie *Uitvoeren* dan wordt het installatiebestand slechts tijdelijk opgeslagen op de computer.
Kiest u voor de optie *Opslaan* dan kunt u een locatie opgeven om het installatiebestand permanent op uw computer op te slaan (totdat u het zelf verwijdert).

U mag kiezen welke optie u verkiest. Ik kies voor de optie *Uitvoeren.*

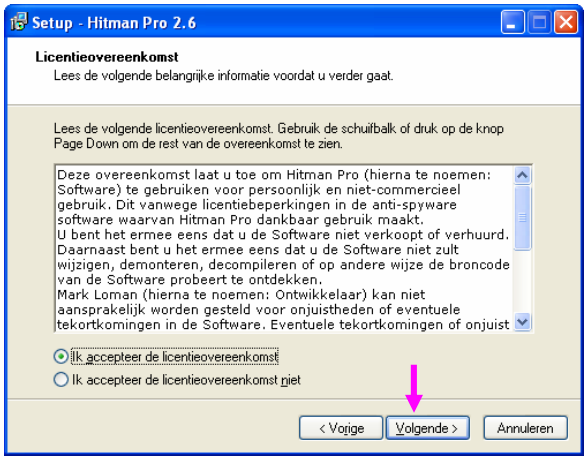
Vervolgens wordt het antispywareprogramma gedownload.

U krijgt nog een beveiligingswaarschuwing. Klik op de knop *Uitvoeren.*

Er verschijnt een dialoogvenster dat vraagt in welke taal u de Setup wilt doorlopen. Selecteer de taal 'Nederlands' in de keuzelijst en druk op de knop.

De wizard van Hitman Pro wordt gestart.

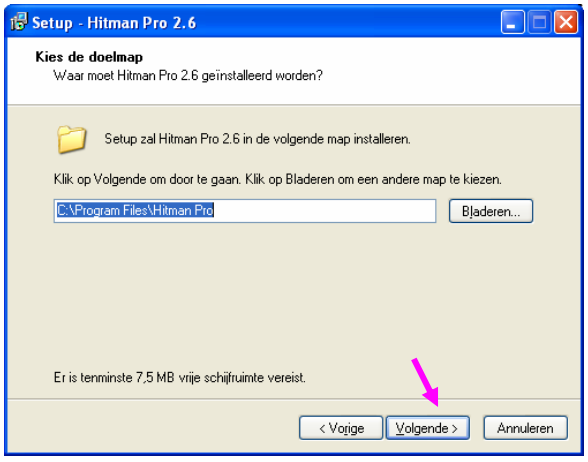
Klik op de knop *Volgende* om verder te gaan met de wizard.



In de tweede stap van de wizard moet u de licentieovereenkomst lezen. Gaat u akkoord, klik dan op de knop *Accept*.

Gaat u niet akkoord met de licentieovereenkomst dan moet u klikken op de knop *Annuleren* waardoor de installatie wordt afgebroken.

Ik ga akkoord met de licentieovereenkomst en klik op de knop *Volgende*.

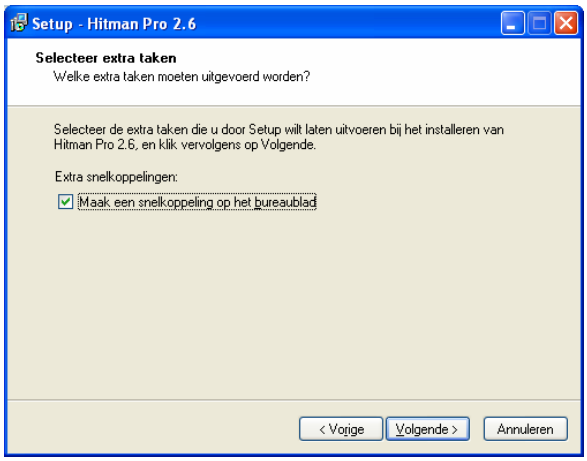


De volgende stap van de wizard vraagt waar Hitman Pro geïnstalleerd moet worden.

Als u een andere locatie wilt opgeven dan de standaard voorgestelde locatie, klik dan op de knop *Bladeren* en selecteer de gewenste locatie.

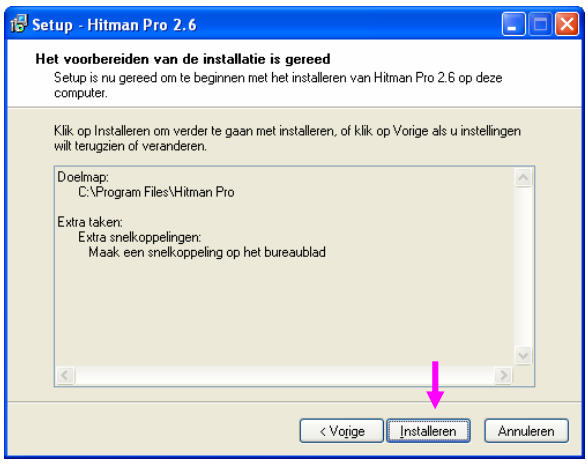
Onderaan het dialoogvenster ziet u dat u tenminste 7,5 MB vrije schrijfruimte nodig heeft om alles te kunnen installeren.

Klik op de knop *Volgende* om naar de volgende stap van de wizard te gaan.



In de vierde stap van de wizard kunt u kiezen of u al dan niet een snelkoppeling van het antispywareprogramma op uw computer wilt plaatsen.

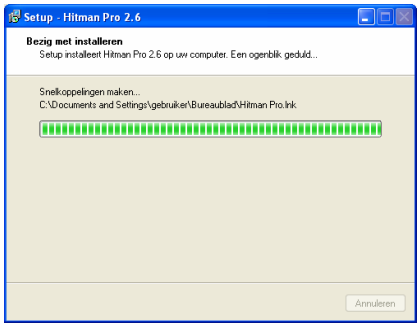
Wilt u geen snelkoppeling op uw bureaublad, vink dan het selectievinkje uit.



Vervolgens krijgt u een samenvatting van de instellingen die u in de setup heeft gekozen.

Gaat u met deze instellingen niet akkoord wijzig die dan door terug te keren in de setup met de knop *Vorige.*

Klik op de knop *Installeren* als u met alle instellingen akkoord gaat.



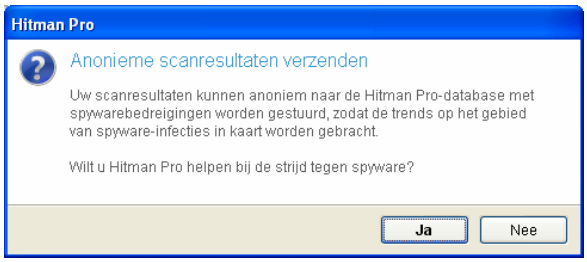
In de vijfde stap van de wizard wordt het antispywareprogramma geïnstalleerd op de computer. U ziet het verloop ervan op uw scherm.

Hierna verschijnt er automatisch een volgend venster dat weergeeft dat de installatie voltooid is.

Laat het selectievinkje in het dialoogvenster aanstaan want zo wordt het programma onmiddellijk gestart na het voltooien van de setup.

Klik op de knop *Voltooien* om de setup af te sluiten.

Sluit de wizard af door op de knop *OK* te klikken.



Hitman Pro wordt geopend.

Eerst krijgt u een venster waarin de vraag wordt gesteld of het programma de gegevens die het verzamelt op uw computer mag doorsturen naar de webserver van Hitman Pro. Dit gebeurt anoniem en u helpt er trouwens het antispywareprogramma mee verbeteren.

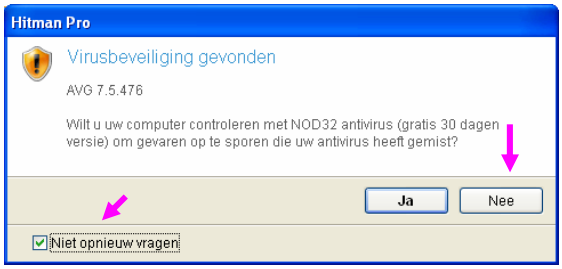
U maakt een keuze door op de *Ja*-knop of de *Nee*-knop te klikken.

U krijgt nu het hoofdvenster van *Hitman Pro* te zien.

In principe moet u niets meer aan de standaardinstellingen veranderen. Wilt u dit toch doen dan kunt u onderaan op de knop *Instellen* klikken.

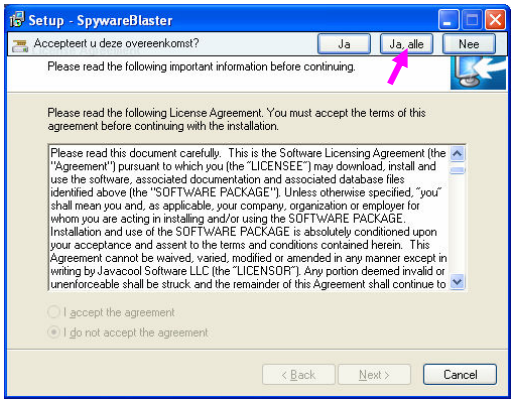
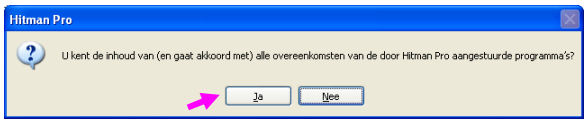
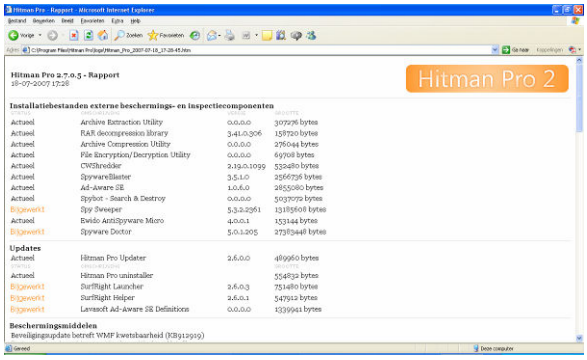
Hitman Pro is nu geïnstalleerd maar de antispywareprogramma's waarvan hij gebruikt maakt, werden nog niet binnengehaald. Wanneer u nu voor de eerste maal klikt op de knop *Start* in de rechterbenedenhoek haalt *Hitman Pro* alle programma's van het internet binnen, stelt de instellingen ervan zelf in en scant uw volledige computer (indien u tenminste in het hoofdvenster niets veranderd heeft) op spyware. Als er spyware gevonden wordt, wordt ze verwijderd. Dit proces kan enkele uren duren en vertraagt de andere bezigheden op uw computer enorm. Het is daarom aan te raden om deze procedure uit te stellen tot u enkele uren uw computer niet nodig heeft.

Tip: Indien u deze procedure 's nachts laat uitvoeren, kunt u er bijvoorbeeld voor kiezen om de computer af te sluiten na deze inspectie. Indien u dit wenst, klik dan het keuzevinkje '*Computer afsluiten na inspectie'* aan in het hoofdvenster van *Hitman Pro.*



Waarschijnlijk krijgt u na het drukken op de knop *Start* dit waarschuwingsvenster. Hitman Pro vraagt of hij het antivirusprogramma NOD32 dertig dagen lang gratis mag gebruiken om computervirussen op te sporen.

Indien u al een goeddraaiend antivirusprogramma heeft, klikt u beter het vinkje aan *Niet opnieuw vragen* en klikt u dan beter op de knop *Nee.* Meerdere antispywareprogramma's op één computer zijn toegelaten

	maar meerdere antivirusprogramma's kunnen met elkaar in conflict gaan met een slecht resultaat als gevolg.
 	Op een gegeven moment zal *Hitman Pro* u vragen of u de gebruikersovereenkomst aanvaardt van een bepaald antispywareprogramma dat *Hitman Pro* gebruikt. Hij zal dit enkele keren vragen. Omdat ik het programma *Hitman Pro* vertrouw, klik ik bovenaan op de knop '*Ja, alle'* waardoor ik in één keer alle overeenkomsten accepteer. Daarna krijg ik wel nog een dialoogvenster waarin ik mijn keuze moet bevestigen; ik klik op de knop *Ja.* Wilt u alle gebruikersovereenkomsten eens nalezen dan moet u één voor één accepteren en klikt u op de knop *Ja* om de gebruikersovereenkomst, die in het venster actief is, te accepteren. Gaat u met een gebruikersovereenkomst niet akkoord dan moet u klikken op de knop *Nee* waardoor u dat programma niet kunt gebruiken (want u gaat niet akkoord met de voorwaarden ervan).
	Nadat *Hitman Pro* de installatie volledig heeft uitgevoerd, krijgt u hierover een rapport te zien. U kunt dit eventueel eens nalezen en vervolgens op de knop *Sluiten* klikken om dit rapport te sluiten. *Hitman Pro* is nu volledig gebruiksklaar. Vergeet niet om toch wekelijks uw computer te scannen op spyware.

5 Onveilig chatten

5.1 Inleiding

Vandaag is de schoolomgeving en de jeugdbeweging niet meer de enige plek waar jongeren vrienden leren kennen en er hun vriendschappen ook onderhouden. Tegenwoordig wordt steeds vaker het internet als de favoriete 'hangplek' van de meeste jongeren gezien.

Jongeren brengen heel wat tijd door achter hun computer en het internet is dan ook een onmisbaar onderdeel van hun sociaal leven geworden. Msn'en doen ze met 'vrienden', via een chatbox praten ze vaak met onbekenden waardoor vriendschappen ontstaan die ze dan via MSN onderhouden.

Vaak zegt men dat u op het internet kunt zijn wie u wilt zijn, dat is ook zo. Denk eraan dat dit ook geldt voor andere mensen die op het internet zitten. Als u aan het MSN'en of aan het chatten bent, weet u dan precies wie er aan de andere kant van de computer zit? Het antwoord is neen, u weet nooit met volledige zekerheid met wie u te maken heeft. Mensen kunnen op het internet een totaal andere identiteit aannemen, zich anders voordoen dan ze in werkelijkheid zijn; iemand van veertig jaar kan zich voordoen als een jongen van twaalf jaar. Let daarom ook op welke informatie u op het internet doorgeeft.

Enkele cijfers over de Belgische chattende jeugd om even over na te denken:

- 25 % van de kinderen (9-14 jarigen) chat met onbekenden.
- 40 % van de jongeren komt via het chatten in contact met choquerende zaken.
- 35 % procent van de meisjes wordt tijdens het chatten op het internet lastiggevallen met seksueel getinte vragen.
- 5% van de chattende jongens en 12 % van de chattende meisjes kreeg in 2006 de vraag om zich uit te kleden voor de webcam.
- In de periode 2003-2004 zijn alleen al in België vierenvijftig dossiers over pedofielen, die via het internet contact zochten met kinderen, doorgegeven aan de Cel Mensenhandel.

5.2 Wat kan er fout lopen in cyberspace

Situatie 1

Vanavond is Magali (16 jaar) goed geluimd. Ze kan eindelijk wraak nemen op Celine. Die is haar ergste vijand geworden sinds ze haar vriendje heeft ingepikt. Haar plan is heel eenvoudig. Ze heeft het bedacht tijdens de internetles op school. Celine zat bij Magali in de buurt zodat ze de loginnaam en het paswoord van Celines e-mailaccount kon zien.

Magali besluit naar de hele klas een e-mailtje te sturen via de account van Celine. En niet zomaar een e-mailtje: een gemeen berichtje, waarin ze zowat iedereen zou uitlachen.

De volgende dag moet Celine bij de directeur komen. Ze wordt aan een kruisverhoor onderworpen. Erger nog: er wordt een brief gestuurd naar haar ouders! Celine zweert dat ze onschuldig is, maar niemand gelooft haar. Een paar dagen later begint het hele spelletje opnieuw. Deze keer wordt Celine voor de hele week van school gestuurd. Thuis is ze helemaal in de war. Haar ouders hebben haar een flinke uitbrander gegeven.

Als straf mag Celine niet meer op de computer. Dat weet Magali natuurlijk niet. Ze blijft mailtjes sturen. De ouders van Celine worden op de hoogte gebracht, maar nu verdedigen ze haar. Celine en haar vader gaan in discussie. Ze willen nakijken wat er op de e-mailaccount van Celine gebeurt.

Ze kunnen haar account echter niet raadplegen: het paswoord werkt niet meer. Dat komt omdat Magali het paswoord veranderde. De vader van Celine stuurt een mailtje naar de

access provider om de account te laten blokkeren. Hij is er nu van overtuigd dat er iets vreemds aan de hand is. Hij dient zelfs een klacht in bij de politie. Het duurt niet lang vóór Magali ontmaskerd wordt. Ze wordt voor altijd van school gestuurd. Bovendien wil niemand van haar vriendinnen nog met haar praten. Ze schaamt zich diep.

Situatie 2

Pedofiel vindt slachtoffertje door chatbox

Het Antwerpse parket heeft een pedofiel opgepakt die via een chatbox contact had gelegd met een dertienjarige. De man bekende dat hij de jongen, die zich had voorgedaan als een zestienjarige, seksueel heeft misbruikt. De verdachte maakte een afspraak met een dertienjarige jongen die zou gezegd hebben dat hij zestien was. De twee hadden een eerste ontmoeting op het middaguur voor het Bouwcentrum in Antwerpen. Lang duurde hun rendez-vous niet, omdat de jongen niet kon blijven. Dus werd een nieuwe afspraak gemaakt. Dit keer had de jongen meer tijd, zodat het tweetal naar de studio van de verdachte trok. Daar hadden ze seksuele contacten. Na de feiten vertelde de jongen dat aan zijn ouders, die de politie inschakelden.

Gazet van Antwerpen, 2002-05-27

Deze twee voorbeelden tonen aan dat het internet en de mensen die er zich op begeven niet altijd te vertrouwen zijn, ook al lijken ze misschien vrienden. Na hoelang met een 'vreemde' chatten, beschouwt u een chatvriend als een gewone goede vriend? Of misschien is er wel iemand op de chat/msn die zich inlogde via de gegevens van jouw beste vriend/vriendin (terwijl hij/zij dat niet is). Opletten geblazen dus in cyberspace.

Wat kan er zoal mislopen in cyberspace?

- U kunt een afspraak maken met iemand die u via het chatten leerde kennen. In werkelijkheid blijkt die persoon niet te kloppen met zijn/haar beschrijving die hij/zij eerder gaf op de chat. In de ergste gevallen kan het een pedofiel en/of ontvoerder zijn.
- Iemand kan uw gegevens gebruiken en in uw naam gemene zaken uitvoeren.
- U kunt een foto, webcamfilmpje,… aan een chatvriend doorsturen die het eventueel bewerkt en doorstuurt naar anderen (buiten uw wil).
- …

5.3 Chatboxen

Wat is chatten precies? Wel, chatten is rechtstreeks via uw computer 'babbelen' (typen) met anderen via het internet. Er zijn open en gesloten chatboxen (websites waarop u kunt chatten). Open chatboxen vindt u op websites. De populairste zijn die van chat.to.be (http://www.chat.to.be) en TMF (http://www.tmf.be) maar ook op tal van andere websites wordt er flink gechat. In open chatboxen vindt u meestal meerdere chatrooms waarin u kunt chatten volgens interesse, leeftijd, woonplaats (vb. *Chatroom West-Vlaanderen, Chatroom Clouseau-fans, Chatroom > 18 jaar, …*). Naast open chatboxen zijn er dus ook gesloten chatboxen. Dit zijn chatboxen die u zelf downloadt zoals MSN of ICQ.

5.3.1 Chatten op open chatboxen

Het allerleukste van chatten is dat u zomaar iemand kunt tegenkomen die u anders nooit in uw leven was tegengekomen. U kunt chatvrienden hebben uit alle hoeken van de wereld. Met een snelle internetverbinding en een goede computer lukt het om met elkaar te chat-

ten. Na de eerste kennismaking kunt u (als u dat tenminste wilt) met elkaar afspreken op een bepaald tijdstip op een bepaalde chatbox; dan is hij/zij er ook en dan kunnen jullie verder chatten.

Dat is toch allemaal leuk! Wat is nu het probleem? Wel, men zegt vaak dat u op het internet kunt zijn wie u wilt zijn want u kunt zich op het internet vermommen als iemand anders. Als u bijvoorbeeld vijfendertig jaar bent, kunt u zich op het internet voordoen als een veertienjarige. Leuk toch? Maar het belangrijke is dat u ook beseft dat andere mensen die op het internet zitten dit ook kunnen doen. Volwassenen kunnen zich als een jongere voordoen en omgekeerd.
Als chatter kunt u hier niet veel aan doen… omdat u de identiteit van de persoon met wie u chat niet kunt controleren. U kunt toch vragen of de persoon met wie u chat een foto van zichzelf doorstuurt? Ja, maar denk eens na… Hoe snel vindt u op het internet een foto van een trendy en goed uitziende jongen/meisje. Zeker bent u op het internet dus nooit. Het is al langer bekend dat niet elke chatter de beste bedoelingen heeft en we weten allemaal al lang dat de cyberwereld niet per se veiliger is dan de echte wereld.

Er zijn toch moderators op een chatbox?

Inderdaad, een moderator is een ervaren chat-kenner die 'alle' gebeurtenissen in de chatroom volgt en erop toekijkt dat iedereen zich aan de regels van de chatbox houdt. Als de moderator vindt dat een bepaalde chatter te ver gaat, kan hij/zij bepaalde mensen de toegang tot een chatroom ontzeggen. Dat kan bijvoorbeeld gebeuren wanneer een chatter zich niet netjes gedraagt tegenover de andere chatters, hen uitscheldt of intimideert. Maar ondanks hun inspanningen kunnen zij niet altijd alles gezien hebben als u bedenkt hoeveel er op een dag gechat wordt.

Wat doet u als u te maken heeft met een vervelende chatter. Enkele tips om onmiddellijk in te grijpen (voor het escaleert en u zich echt 'bedreigd' voelt in uw eigen omgeving).

- Reageer niet.
- Blokkeer de chatter. Wanneer u een chatter blokkeert, ziet hij in zijn/haar lijstje dat u niet meer in de chatbox bent. U bent in zijn ogen offline; ook al is dit niet zo. Op die manier kan de chatter langs die weg geen contact meer met u opnemen zolang u zijn/haar blokkering niet opheft. Hoe u iemand blokkeert, hangt af van chatbox tot chatbox en ook niet op alle open chatboxen heeft u een blokkeermogelijkheid.
- Verwittig de moderator van de chatbox over het gedrag van de chatter.
- Zeg tegen uw chatvrienden dat die bepaalde persoon niet te vertrouwen is.
- U kunt ook een andere nickname gebruiken zodat die vervelende chatter niet weet dat u nog/terug op de chat bent.

Het is dus aan te raden vooraleer u chat, te kijken of er een moderator aanwezig is in de chatbox of chatroom. Controleer ook even of u een chatter al dan niet kunt blokkeren en hoe u dat precies doet.

5.3.2 Chatten op gesloten chatboxen

De bekendste gesloten chatbox is MSN Messenger. Dit is de officiële naam van het instant messaging programma maar iedereen noemt het kortweg msn'en. Er zijn natuurlijk nog andere gesloten chatboxen zoals ICQ maar die komen we steeds minder tegen in de populaire msn-wereld. Gesloten chatboxen moet u downloaden van het internet. In 1, 2, 3 staat het programma op uw computer en kunt u chatten met uw 'vrienden'.

Een gesloten chatbox is iets 'veiliger' dan een open chatbox want u bepaalt wie er in uw chatlijst komt. U moet iemand 'accepteren' om hem/haar toe te voegen aan uw chatlijst. Het veiligste is om enkel de mensen in uw chatlijst op te nemen die u goed kent en die u vertrouwt (ook al is vertrouwen op het internet een relatief begrip). Maar zeg nu zelf, kent u iedereen 'persoonlijk' die in uw chatlijst staat? De meeste jongeren streven ernaar om een lange chatlijst op te bouwen, omdat ze op die manier meest kans hebben dat er iemand online is als ze willen msn'en. Maar vaak zitten er in die msn-lijst 'onbekenden' die ze op een open chatbox hebben ontmoet.

Meestal meldt iemand zich met zijn of haar hotmailadres. U moet die persoon dan 'accepteren', maar…

- iemand kan zich met zijn/haar e-mailadres voordoen alsof hij/zij uw vriendje of vriendinnetje is…;
- iemand kan vervelend gaan doen, terwijl hij in uw chatlijst staat…;
- iemand kan rare foto's, filmpjes, … sturen, soms met een computervirus erin…;

En dan zit u er maar mooi mee… Een gesloten chatbox is redelijk veilig: tenminste als u het vergelijkt met een open chatbox via een website. Daarop kan namelijk iedereen met u chatten. Bij een gesloten chatbox moet u eerst bepalen of u die bepaalde persoon in uw chatlijst al dan niet opneemt. Dat is het mooie eraan. Maar soms krijgt u later spijt dat u iemand heeft opgenomen in de chatlijst van uw gesloten chatbox. Daar kunt u wat aan doen: Hoe? Blokkeren en/of verwijderen!

Doet er iemand uit uw msn-lijst vervelend tegen u? Wat kunt u doen? Enkele tips…

- Reageer er niet op.
- Blokkeer die persoon!
- Blokkeer die persoon meteen in uw e-mailprogramma (raadpleeg hiervoor de helpfunctie van uw e-mailprogramma).
- Praat er eens over met vrienden, vriendinnen of ouders. Vraag steun want u bent tenslotte zwaar ontgoocheld in een persoon die u vertrouwde (anders zou u hem niet in uw chatlijst toelaten).

5.4 Wat als het uit de hand loopt?

Wat als het echt uit de hand loopt? U wordt gepest, bedreigd, u voelt zich misbruikt, … In een chatsessie hoeft u niet alles te pikken en gaan anderen soms echt te ver. Maar wat moet u dan precies doen?

- Bij een open chatbox meldt u de klacht bij de moderator of beheerder van de chatroom.
- Bij een gesloten chatbox kunt u uw klacht melden bij de helpdesk van de open chatbox die u gebruikt. Bij MSN: http://groups.msn.com/feedback.msnw. Nog beter is om uw klacht te mailen naar clicksafe@childfocus.org
- Uw klacht kan ook zo ernstig zijn dat het belangrijk is om aangifte te doen bij de politie; doe dit dan ook. Ook cybercriminelen mogen niet ongestraft verder blijven werken.

Welke informatie heeft u nodig bij een klacht?

- Noteer de nickname en het e-mailadres van de persoon die u lastigvalt.
- Heel belangrijk is dat u datum en tijd van het chatgesprek noteert.
- Noteer de naam of het webadres van de chatroom.

- Verzamel alle informatie die u heeft van de persoon die u lastigvalt (eerdere chatgesprekken, foto's, filmpjes, persoonlijke gegevens van die persoon, …)
- Neem een schermafdruk (als bewijs) van de onaangename zaken die de chatter zegt of doet. Een schermafdruk neemt u door één keer te drukken op de Prt Scr-toets (Print Screen) op uw toetsenbord. Open bijvoorbeeld het programma Word en kies voor Bewerken, Plakken. Uw schermafdruk wordt in het document geplaatst. Sla het document op en druk het eventueel af.

5.5 'Veilig' chatten

De overheid en de overkoepelende organisatie van de internet service providers ISPA zijn zich bewust geworden van de gevaren die in het chatten schuilen en hebben gezamenlijk het proefproject *SaferChat* (vertaald: veilig chatten) opgericht. Dit proefproject is gericht naar jongeren tussen twaalf en vijftien jaar die een elektronische identiteitskaart (afkorting: eID) op zak hebben.

Wat is een elektronische identiteitskaart?

De elektronische identiteitskaart (eID) vervangt de klassieke identiteitskaart. Ten laatste in 2009 moeten alle Belgen er eentje hebben. De eID heeft het formaat van een bankkaart en biedt interessante en vernieuwende gebruiksmogelijkheden. De eID bevat niet alleen persoonlijke gegevens zoals uw naam en voornamen, plaats en datum van geboorte, nationaliteit en geslacht, maar ook een computerchip. Dankzij die chip kunt u bewijzen wie u bent via de computer en het internet. (Meer informatie over de eID vindt u op http://eid.readers.belgium.be).

Voortaan kunnen jongeren dus chatten in speciale chatrooms bedoeld voor jongeren tussen 12 en 15 jaar. Deze chatrooms zijn speciaal beveiligd. U moet uw eID in een kaartlezer (Een kaartlezer is een apparaatje dat uw eID met uw pc verbindt. Meer informatie over de kaartlezers vindt u op de website: http://www.cardreaders.be/nl.) stoppen en uw geheime eID-pincode invoeren. Men controleert dan (aan de hand van uw rijksregisternummer) of u effectief wel tussen de twaalf en de vijftien jaar bent en of de eID-pincode correct is. Kloppen uw gegevens dan krijgt u toegang tot de chatroom. Het resultaat is dat u zich geen zorgen meer hoeft te maken over de ongewenste aanwezigheid van volwassenen die zich voordoen als een leeftijdsgenoot.

Voorlopig zijn er al drie beveiligde chatrooms die enkel en alleen toegankelijk zijn voor jongeren tussen de twaalf en vijftien jaar. Eén van de drie chatrooms is enkel toegankelijk voor meisjes, een andere enkel voor jongens en een derde is voor zowel jongens als meisjes. Goed om weten is dat er in de beveiligde chatrooms toezicht wordt gehouden door moderatoren. Zij zijn de enige volwassenen die kunnen volgen wat er in de chatrooms gebeurt.

Toch is dit systeem nog niet waterdicht en is het nog steeds opletten geblazen. Enkele lekken in de 'veilige' chatrooms:

- Nog niet alle Belgische chatsites worden afgeschermd met eID.
- Ook leeftijdsgenoten kunnen heel kwetsend overkomen op cyberspace. Ze beseffen vaak niet dat er in de cyberwereld ook echte gevoelens bij te pas komen. We zijn tenslotte geen robots maar mensen van vlees en bloed.
- Bij buitenlandse chatsites is er nog geen sprake van afscherming aan de hand van eID (België is het eerste land).
- Pedofielen kunnen bijvoorbeeld de eID van hun kinderen gebruiken om toegang te krijgen tot de chatbox.

Ondanks de lekken in het systeem werd met dit initiatief een belangrijke stap gezet in het veiliger maken van het internet voor jongeren. Als het proefproject succes heeft, komen er ook SaferChat-kamers voor andere leeftijdscategorieën.

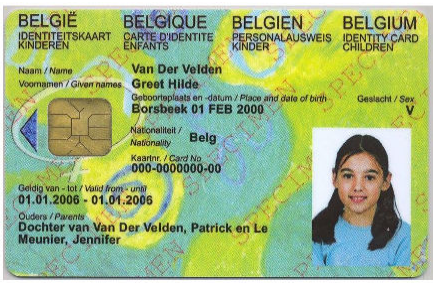
Zijn er chatregels op deze beveiligde chatrooms? Ja, als u wilt chatten in een speciaal beveiligde chatroom moet u, net zoals voor andere chatrooms, bepaalde regels naleven. Deze chatregels bepalen niet alleen wat u zelf mag en niet mag, maar zeggen ook welke rechten u heeft. U vindt ze terug bij de betreffende chatroom. Ze zijn erg belangrijk. Lees ze dus aandachtig vooraleer u begint te chatten.

De eID staat garant voor een ongekend hoge beveiliging want …

1 Het is onmogelijk om de eID na te maken.

2 De eID wordt na diefstal of verlies onbruikbaar gemaakt, op dezelfde manier als dat voor een bankkaart gebeurt. Het is daarom belangrijk dat, wanneer u uw kaart verliest, u dit onmiddellijk meldt aan de overheid (via de website http://www.eid.belgium.be of telefonisch via de eID cardstop: 02 518 21 17).

3 Er is een extra beveiliging onder de vorm van een pincode (net zoals bij een bankkaart) → eID-pincode.



Via onder andere onderstaande websites kunt u eventueel toegang krijgen tot de drie beveiligde chatrooms.

- http://www.chat.be
- http://www.kidcity.be
- http://breedband.telenet.be
- http://place.to.be
- http://www.krey.net/saferchat

5.6 Belangrijke chattips

Chatkanalen en het internet zijn fantastische communicatie- en informatiemedia. Wilt u er ten volle van kunnen genieten, dan doet u er goed aan om enkele veiligheidsrichtlijnen in acht te nemen.

1 Geloof niet alles wat in de chatroom wordt verteld. Sommige mensen vinden het leuk om te liegen als ze zich kunnen verschuilen achter een schuilnaam. Soms zijn het onschuldige leugentjes, maar soms zit er meer achter. Het is dus verstandig om uw chatvrienden niet meteen in vertrouwen te nemen. Waarmee niet bedoeld wordt dat de chat een verzamelplaats is voor voltijdse leugenaars.

2 Geef niet meteen uw telefoonnummer, e-mailadres en woonplaats aan een chatgenoot. Wacht daarmee tot u hem/haar beter kent en het gevoel heeft dat u hem/haar kunt vertrouwen. Wees altijd voorzichtig. Er zijn verhalen bekend van pedofielen die geduldig contacten opbouwen met jongeren via de chat en pas maanden na de kennismaking vragen om een afspraakje in levende lijve. Waarmee niet gezegd wordt dat chatten altijd een anonieme aangelegenheid moet blijven. De chat is een leuke manier om elkaar te leren kennen. Tenminste, zolang het op een eerlijke manier gebeurt.

3 Gebruik minimum twee e-mailadressen. Maak een e-mailadres aan dat u enkel en alleen gebruikt voor uw goede vrienden die u kent van bijvoorbeeld op school, in de jeugdbeweging, … Maak een ander e-mailadres (plaats uw echte naam niet in het e-mailadres) aan dat u gebruikt voor 'onbekenden' en voor wanneer u een formulier moet invullen op het internet. Wanneer het tweede e-mailadres overspoeld wordt met e-mails

die u absoluut niet leuk vindt, kunt u ervoor kiezen om dit e-mailadres niet meer te gebruiken en een ander te maken.

4 Uw paswoord is geheim. Uw password is alleen van u, vertel het dus aan niemand. Voordat u het weet, kent iedereen het en kunnen andere mensen dan binnen in uw persoonlijke zaken op het internet zoals e-mails, chat, profielsite (bijvoorbeeld www.redbox.be). Mensen die uw paswoord kennen kunnen ook in uw naam chatten met iemand anders of e-mails sturen. Denk maar terug aan het verhaal van Celine en Magali.

5 Strooi de persoonlijke gegevens van uw vrienden niet in het rond op de chat. Dat is niet netjes, het getuigt van een totaal gebrek aan respect voor hun privacy en het kan hen, in het ergste geval, zelfs in gevaar brengen. Wat zou u er zelf van vinden als u ineens vervelende e-mails en sms-berichten van onbekenden zou krijgen omdat uw vrienden op straat kaartjes hebben uitgedeeld met uw foto, telefoonnummer en e-mailadres erop? Inderdaad, u zou het niet leuk vinden en u zou zich zorgen maken. Waarmee we niet willen zeggen dat het verboden is om mensen met elkaar in contact te brengen via de chat. Doe het alleen niet zonder dat de ander ermee instemt.

6 Ga geen blind date aan met iemand die u pas heeft leren kennen via de chat. De kans bestaat immers dat die persoon niet is wie hij/zij beweert te zijn. Dat hebben we wel geleerd uit de afschuwelijke verhalen over pedofielen die via chatboxen contact zoeken met jongeren. Waarmee we niet willen zeggen dat afspraakjes met chatvrienden uit den boze zijn. Maar let op! Spreek af op een openbare plaats waar veel mensen aanwezig zijn en neem desnoods een vriend/vriendin mee. Zorg ervoor dat uw ouders ook weten waar en met wie u op stap bent.

7 Verwittig uw ouders wanneer een chatvriend dingen wil die u verdacht of niet leuk vindt. Leg hen uit wat die chatvriend wil of vraagt. Luister naar hun goede raad. Vertrouw op hun inschattingsvermogen. U moet trouwens ook luisteren naar uw eigen gevoel en steunen op uw eigen kennis. Alleen kunt u niet ontkennen dat uw ouders al meer hebben meegemaakt dan u, waardoor ze sommige situaties ook beter kunnen inschatten.

8 Signaleer een verdachte chatter meteen aan al uw chatvrienden. Als blijkt dat die chatter ook anderen een slecht gevoel bezorgt, weet u dat uw vermoedens gerechtvaardigd zijn. In dat geval dient uw signalement ook als een waarschuwing voor chatters die nog niet door de valse vriend zijn aangesproken. Als blijkt dat u de enige bent die onraad ruikt, heeft u alle tijd om uw vermoedens nog eens op een rijtje te zetten en eventueel uw mening te herzien. Iedereen vergist zich wel eens. Daar hoeft u zich niet voor te schamen.

Wie is verdacht?

a Iemand die op de chat op alle mogelijke manieren probeert om uw naam, gsm-nummer en andere persoonlijke informatie te achterhalen (ook al heeft u hem/haar laten weten dat u die informatie niet wilt geven).

b Iemand die uw paswoord vraagt of probeert te raden. Uw paswoord is strikt vertrouwelijk en dus voor niemand anders bestemd. Er is geen enkele geldige reden waarom u het aan iemand zou moeten toevertrouwen. Doe het dan ook niet!

c Iemand die vraagt om uw chatvriendschap met hem/haar geheim te houden. Stel uzelf de vraag: waarom zou die vriendschap geheim moeten zijn? Heeft uw chatvriend misschien wat te verbergen?

9 Laat u niet doen. Op de chat beslist u, en u alleen, wat er gebeurt. Niemand heeft het recht om te zeggen wat u moet doen. Als een van uw chatvrienden dat toch probeert, is het geen echte vriend. Meer nog, de kans is reëel dat die persoon u in de val probeert te lokken. Wanneer u met vervelende sms-berichten gepest wordt door onbekenden

nadat u zonder nadenken uw gsm-nummer aan chatvrienden heeft gegeven, kan de gsm-operator nagaan wie de berichten heeft verstuurd om de pesterijen te doen stoppen. Wanneer u met vervelende e-mails gepest wordt, kunt u makkelijk alle berichten van de (anonieme) pestkop laten blokkeren vooraleer ze in uw mailbox belanden. Het volstaat om in uw e-mailprogramma aan te duiden van wie u geen berichten meer wilt ontvangen. Reageer dus nooit op iemand die u online een ongemakkelijk gevoel geeft of van streek maakt. Praat er thuis over, ook als u gemene of onbeschofte e-mails krijgt.

10 Blijf beleefd. Het is niet omdat iedereen op de chat een schuilnaam gebruikt, dat het geen echte mensen zijn met menselijke gevoelens. Het is niet omdat u elkaar op de chat niet in de ogen kijkt, dat u de regels van beleefdheid en goed fatsoen moet negeren. Op de chat kunt u naar hartelust schelden en vuile praat verkopen, want niemand weet wie u bent. Vindt u dat cool en spannend? Sorry, maar dan bent u verkeerd bezig. Denk eens hoe u zelf behandeld zou willen worden.

11 Let op wat u doet voor een webcam. Reageer niet op uitnodigingen om naakt te poseren voor uw webcam. Ook niet als u hiervoor geld krijgt aangeboden. De persoon aan de andere kant van de computer kan van deze beelden foto's en/of filmpjes maken. Voor u het weet, zweven deze zaken voorgoed op het internet en krijgt u spijt van uw daden. Laat u dus niks wijsmaken en laat u niet domineren en/of chanteren. Weet dat er instanties zijn die u te hulp schieten bij dergelijke chantage.

5.7 Besluitvorming

In dit deel werd aangetoond dat het heel belangrijk is om op te letten in de cyberwereld. Voor u het weet loopt het mis… Velen zijn zich hiervan nog niet genoeg bewust. Denk er aan dat achter elke computer een persoon zit die ook zijn/haar gevoelens heeft. Behandel iedereen zoals u zelf behandeld wilt worden.

Als u constant door een chatvriend lastig gevallen wordt (pesterijen, bedreigingen, …), neem dit dan serieus. Vaak vegen we deze zaken weg met te zeggen: "het is maar op het internet, hij/zij kan mij toch niets maken". Let op, voor u het weet staat hij/zij aan uw voordeur of aan de schoolpoort. Geef dus uw persoonlijke gegevens niet bloot. Chat uzelf niet bloot!

6 Cyberpesten

6.1 Definitie

Cyberpesten is een relatief nieuw fenomeen. Volgens Bill Belsey kunnen we cyberpesten als volgt definiëren: 'het gebruik van informatie- en communicatietechnologieën (zoals e-mail, gsm, chatboxen, persoonlijke websites, forums, …) om doelbewust, herhaaldelijk en vijandelijk gedrag bij een individu of een groep te steunen, dat de intentie heeft om anderen te kwetsen'.

Bij het gebruik van informatie- en communicatietechnologieën wordt de non-verbale communicatie tot een minimum herleid: gebaren, gelaatsuitdrukkingen, ondertonen bereiken de ontvanger zelden. We kunnen dus stellen dat er bij cyberpesten een verhoogde, om maar niet te zeggen grote, kans bestaat op misinterpretatie bij de ontvanger.

Bij cyberpesten is dus het herhaaldelijk karakter belangrijk. Hieronder kunnen we verstaan: regelmatig pestgedrag op chatboxen, regelmatig verwijtende e-mails, websites met kwetsende foto's die een lange tijd op het internet beschikbaar blijven, kwetsende en verwijtende uitspraken die op een forum staan, …

Om te cyberpesten hoeft u fysiek niet sterk te zijn, wel moet u 'goed' kunnen werken met de complexe nieuwe technologieën en deze kunnen manipuleren. Concreet betekent dit dat personen die in dagelijkse face-to-face situaties omwille van hun fysieke of persoonlijkheidskenmerken een hogere kans hebben om slachtoffer te worden van pesterijen, in de cyberwereld pesters kunnen zijn (als ze over de nodige digitale vaardigheden beschikken). Soms gebruikt men wel de term 'technopower' waarmee men bedoelt dat de macht van een persoon in cyberspace afhangt van hoe goed hij/zij kan omgaan met complexe nieuwe technologieën en deze kan manipuleren.

U kunt trouwens niet alleen gecyberpest worden door mensen uit uw omgeving, maar u kunt ook gecyberpest worden door mensen die u online heeft ontmoet en die u in werkelijkheid nog nooit gezien heeft of waarvan u hun echte identiteit niet kent. Het is typerend voor de nieuwe ICT dat mensen anoniem kunnen werken, dus zonder hun echte identiteit te onthullen.

Bij cyberpesten is er dus geen sprake van persoonlijke fysieke pesterijen. U kunt bijvoorbeeld niet in elkaar geslagen worden door middel van de nieuwe communicatie- en informatietechnologieën, maar soms zijn de emotionele vernederingen nog veel erger en constanter.

6.2 Vormen van cyberpesten

Net zoals bij het traditioneel pesten kan er bij cyberpesten een onderscheid gemaakt worden tussen directe en indirecte vormen van pestgedrag.

Als we praten over direct pesten betekent dit dat het slachtoffer onmiddellijk bij het pesten betrokken is. Praten we over indirect pesten dan is het medeweten van het slachtoffer van de pesterijen niet noodzakelijk vereist.

6.2.1 Direct cyberpesten

Het directe cyberpesten kunnen we indelen in vier categorieën. Bij elke categorie enkele voorbeelden:

- Fysiek cyberpesten
    - Computervirussen doorsturen waardoor de computer van de virusontvanger(s) schade oploopt.
    - Het e-mailadres van iemand hacken en zijn/haar paswoord veranderen waardoor die persoon moeilijk of geen toegang meer heeft tot zijn/haar e-mailaccount.
    - Het versturen van enorm veel bestanden of van grote bestanden via e-mail. Hierdoor raakt de mailbox van de ontvanger vol en kan hij/zij (tijdelijk) geen e-mails meer ontvangen.
    - Iemands computer hacken om private of vertrouwelijke informatie te bekomen.
- Verbaal online pesten
    - Flaming, het gebruik van verbaal geweld bij internet- of e-mailverkeer.
    - Seksueel vernederende boodschappen versturen en/of publiceren.
- Non-verbaal online pesten
    - Bedreigende, pornografische en vernederende foto's / illustraties / cartoons van iemand doorsturen naar die persoon (al dan niet bewerkt).
    - Pornografische beelden en/of foto's van iemand doorsturen naar die persoon (al dan niet bewerkt).
- Sociaal online pesten
    - Uitsluiting uit online groepen.

6.2.2 Indirect cyberpesten

Enkele voorbeelden van indirect cyberpesten:

- Outing (iets openbaar bekend maken)
    - Private of gênante informatie over iemand verspreiden via e-mail, chatgesprekken, SMS, …
    - Bedreigende, pornografische en vernederende foto's / illustraties / cartoons van iemand publiceren op het internet zodat anderen ze kunnen zien (al dan niet bewerkt).
    - Een online privégesprek met een persoon laten lezen door anderen.
- Happy Slapping; dit staat voor het nieuwe fenomeen waarbij meestal een groepje jongeren één iemand (een zwakkere) in elkaar slaat. Dit geweld wordt gefilmd (meestal met de videocamera van een gsm) en wordt op het internet geplaatst.
- Masquerade
    - De elektronische identiteit van een slachtoffer overnemen door zich als die persoon voor te doen in chatboxen, forums, pornografische websites, …
    - Het e-mailadres van iemand hacken en obscene of beledigende berichten versturen naar zijn of haar contactpersonen in zijn of haar naam.
    - Iemand voor een wedstrijd, activiteit of voor een nieuwsbrief inschrijven zonder dat die persoon hiervan op de hoogte is of zonder dat hij/zij dat wil (bv. nieuwsbrief van een pornografische website).
- De reputatie van iemand besmeuren door geruchten en/of leugens te verspreiden over die persoon via e-mail, chatgesprekken, SMS, …

- Beledigende en/of vernederende boodschappen over een persoon op een website, gastenboek, blog, … plaatsen.
- Populariteitstesten over een bepaalde persoon (meestal een minder populair iemand) op een website plaatsen.

6.3 Rollen bij cyberpesten

6.3.1 De cyberpesters

Onderzoekers Ybarra en Mitchell (2004b) deden onderzoek naar internetpesterijen en hun relatie met andere factoren. Uit hun onderzoek enkele opmerkelijke besluiten over cyberpesters:

- Er bestaat een verband tussen pestgedrag en een slechte emotionele band tussen opvoeder(s) en jongere(n). Cyberpesters staan minder onder toezicht van hun ouders, maar ze worden meer gestraft.
- Jongeren die psychosociale moeilijkheden hebben, hebben meer kans om een cyberpestkop te worden.
- Ongeveer de helft van de cyberpesters zijn slachtoffers van traditioneel pesten.
- Cyberpesters vertonen meer depressieve symptomen en hebben meer kans op slechte schoolresultaten dan traditionele pestkoppen.
- Cyberpesters vertoeven minstens 4 keer per week op het internet.
- Cyberpesters bezoeken vaker chatrooms dan andere jongeren.
- Cyberpesters maken vaak duidelijk dat het internet heel belangrijk is voor hen.
- Cyberpesters schatten hun kennis over het internet hoger in dan andere jongeren.
- Er zijn evenveel jongens als meisjes die cyberpesten.
- Oudere kinderen zijn vaker cyberpesters dan jongere kinderen.

6.3.2 De cybergepesten / de cyberslachtoffers

De onderzoekers Ybarra en Mitchell (2004b) deden ook onderzoek naar de slachtoffers van cyberpesten. Uit hun onderzoek enkele belangrijke besluiten over cybergepesten:

- Veel jongeren die via het internet gepest worden, zijn ook het slachtoffer van traditionele pesterijen. Toch worden sommige jongeren ook enkel op het internet gepest.
- Ongeveer 69 % van de cyberslachtoffers weten niet wie de dader is. De identiteit van de cyberpester is dus vaak voor hen onbekend.

6.4 Cyberpesten bij Vlaamse jongeren

Door een samenwerking tussen het Vlaams Instituut voor Wetenschappelijk en Technologisch Aspectenonderzoek en een onderzoeksploeg van de Universiteit Antwerpen werd een onderzoek uitgevoerd naar cyberpesten bij Vlaamse jongeren. Deze steekproeftrekking gebeurde bij een populatie van Vlaamse schoolgaande jongeren van het vijfde leerjaar tot en met het zesde middelbaar anno 2005.

Voor de secundaire scholen verliep de steekproeftrekking als volgt: uit elk van de vijf provincies werden (willekeurig) zes scholen gekozen: telkens twee scholen met een ASO-

opleiding, twee scholen met een TSO/KSO-opleiding en twee scholen met een BSO-opleiding. Binnen elk onderwijstype werd bij de ene school de vragenlijst afgenomen in het eerste, derde en vijfde jaar en bij de andere school binnen hetzelfde onderwijstype in het tweede, vierde en zesde jaar. In totaal werden duizend vierhonderdzestien jongeren ondervraagd in het secundair onderwijs, dit gespreid over vierentachtig klassen.

Zowel voor het vijfde als voor het zesde leerjaar werden tien scholen gekozen uit de hele populatie van scholen in Vlaanderen. In deze scholen werden telkens alle leerlingen uit het vijfde leerjaar of alle leerlingen uit het zesde leerjaar bevraagd. In totaal vulden zeshonderdzesendertig lagere schoolkinderen uit twintig verschillende scholen de vragenlijst in.

De bevraging had betrekking op de ervaringen die de kinderen/jongeren hadden in de laatste drie maanden. Hieronder volgen enkele algemene conclusies die ik genomen heb uit het onderzoek.

6.4.1 Slachtoffer van cyberpesten

Uit onderzoek naar cyberpesten werden volgende conclusies getrokken over de Vlaamse cyberslachtoffers:

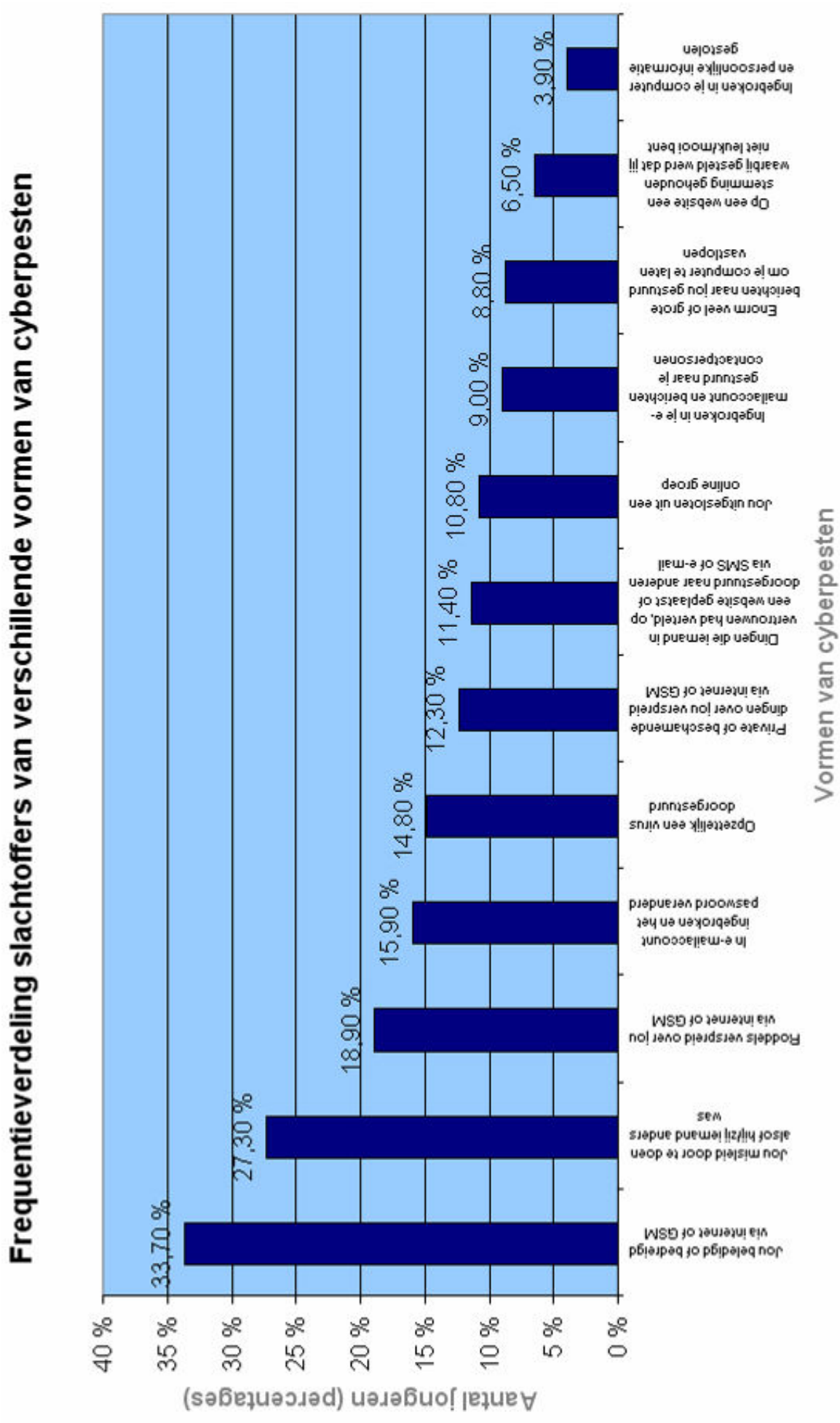
- hebben een grotere internetafhankelijkheid;
- hebben een negatiever zelfbeeld wat betreft sociale vaardigheden;
- zijn vaak ook daders van cyberpesten;
- zijn vaak ook slachtoffers van traditioneel pesten;
- zijn niet zo vaak dader van traditioneel pesten;
- 50 % vertelt aan niemand dat ze gecyberpest worden/werden;
- vertonen meer stress-symptomen.

Hieronder volgen enkele puntjes die nog meer informatie blootgeven over de Vlaamse slachtoffers van cyberpesten.

6.4.1.1 Vormen van cyberpesten waarvan men slachtoffer werd

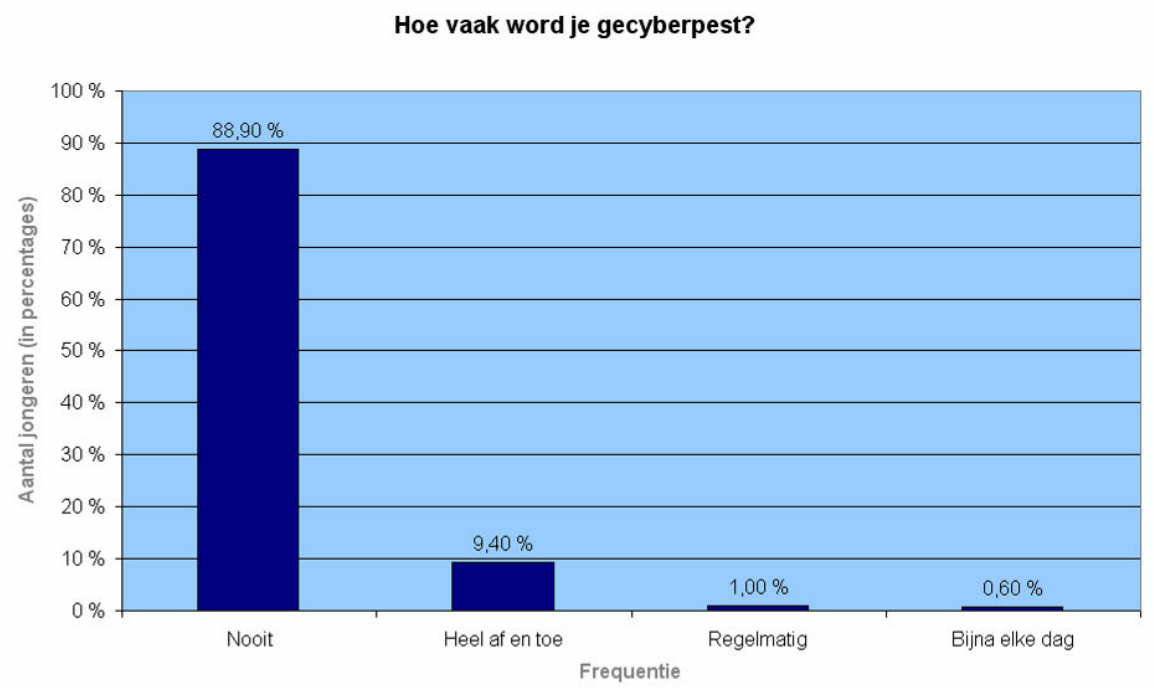
Tijdens het onderzoek kregen de jongeren heel wat vragen voorgeschoteld zoals: "Heeft iemand jou al beledigd of bedreigd via internet of gsm?". In onderstaande grafiek vindt u enkele vormen van cyberpesten terug met het daarbijhorende percentage jongeren dat reeds van deze vorm van cyberpesten het slachtoffer was.

De meest voorkomende vormen van cyberpesten staan vooraan in de grafiek, de minst voorkomende vormen van cyberpesten (bij de jongeren die ondervraagd werden) komen achteraan voor in de grafiek. Van meest voorkomend naar minst voorkomend dus.


Frequentieverdeling slachtoffers van verschillende vormen van cyberpesten
Aantal jongeren (percentages)
0 %
5 %
10 %
15 %
20 %
25 %
30 %
35 %
40 %
33,70 %
27,30 %
18,90 %
15,90 %
14,80 %
12,30 %
11,40 %
10,80 %
9,00 %
8,80 %
6,50 %
3,90 %
Vormen van cyberpesten
Jou beledigd of bedreigd via internet of GSM
Jou misleid door te doen alsof hijzij iemand anders was
Roddels verspreid over jou via internet of GSM
In e-mailaccount ingebroken en het paswoord veranderd
Opzettelijk een virus doorgestuurd
Private of beschamende dingen over jou verspreid via internet of GSM
Dingen die iemand in vertrouwen had verteld, op een website geplaatst of doorgestuurd naar anderen via SMS of e-mail
Jou uitgesloten uit een online groep
Ingebroken in je e-mailaccount en berichten gestuurd naar je contactpersonen
Enorm veel of grote berichten naar jou gestuurd om je computer te laten vastlopen
Op een website een stemming gehouden waarbij gesteld werd dat jij niet leuk/mooi bent
Ingebroken in je computer en persoonlijke informatie gestolen

6.4.1.2 Frequentie van cyberpesten waarbij men slachtoffer was

In de vragenlijst bevroeg men de jongeren ook over hoe vaak ze in de afgelopen drie maanden gecyberpest werden. In onderstaande grafiek vindt u de antwoorden.



6.4.1.3 Door wie wordt men gecyberpest?

Aan de jongeren die gecyberpest werden, vroeg men via de vragenlijst wie de dader was. De jongeren konden meerdere antwoordmogelijkheden aanstippen omdat men mogelijk door meerdere daders gecyberpest werd. Hieronder volgen de resultaten:

- 14,1 % werd gecyberpest door iemand die ze alleen via het internet kennen.
- 44,8 % werd gecyberpest door mensen die hij/zij ook in de echte wereld kennen. (In 57,3 % van deze gevallen wordt men door dezelfde mensen ook traditioneel gepest.)
- 48,5 % werd gecyberpest door onbekenden.

6.4.1.4 Reageren de Vlaamse slachtoffers tegen cyberpesterijen?

In de vragenlijst besteedde men ook aandacht aan de vraag of slachtoffers reageerden op de cyberpesterijen en hoe ze reageerden. Hieronder volgen de resultaten (men kon meerdere mogelijkheden aanduiden).

- 55,1 % vertelde niemand dat hij/zij gecyberpest werd.
- 70,6 % verdedigde zich in de echte wereld.
- 67,4 % blokkeerde de dader op MSN
- 57,6 % vroeg in de echte wereld aan de dader om ermee te stoppen.
- 53,4 % vroeg via het internet aan de dader om ermee te stoppen.
- 50,5 % cyberpestte de dader terug.
- 60,8 % deed alsof er niets gebeurd was.
- 57,3 % wachtte tot het vanzelf zou over gaan.
- 25,0 % gaf zichzelf de schuld.

6.4.2 Dader van cyberpesten

Uit onderzoek naar cyberpesten werden volgende conclusies getrokken over de Vlaamse daders van cyberpesten:

- besteden veel tijd op het internet;
- kunnen op minder betrokkenheid van hun ouders rekenen als het aankomt op internetgedrag en/of internetcontrole;
- zijn vaak ook slachtoffer van cyberpesten;
- zijn vaak ook dader van traditioneel pesten;
- pesten anoniem (7 op 10 daders).

Een vraag die op de lippen van vele mensen ligt en die onderzocht werd: 'Zijn er onder de cyberpesters relatief meer (zware) gebruikers van (gewelddadige) videogames of computergames te vinden?' Uit het onderzoek blijkt dat er geen verband is tussen het daderschap van cyberpesten en de voorkeur voor gewelddadige videogames of computergames.

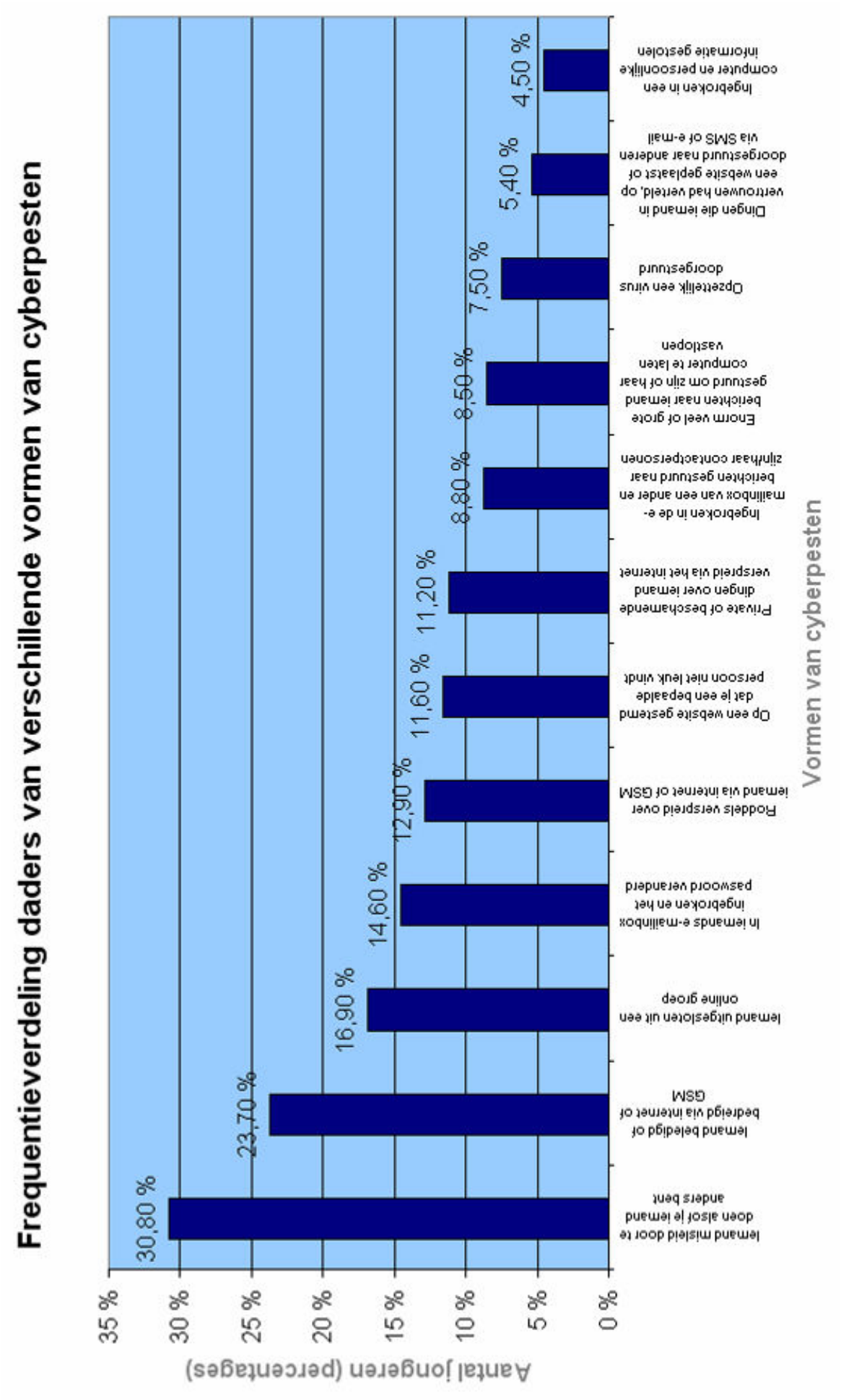
De Vlaamse cyberpesters vonden hun daden 'grappig'. Meestal zijn de cyberdaders zich ook niet bewust van het effect van hun gedrag op hun slachtoffers, omdat er een gebrek is aan visuele feedback van het slachtoffer.

Hieronder volgen nog enkele puntjes die nog meer informatie over de Vlaamse cyberpesters prijsgeven.

6.4.2.1 Vormen van cyberpesten waaraan men zich schuldig maakte

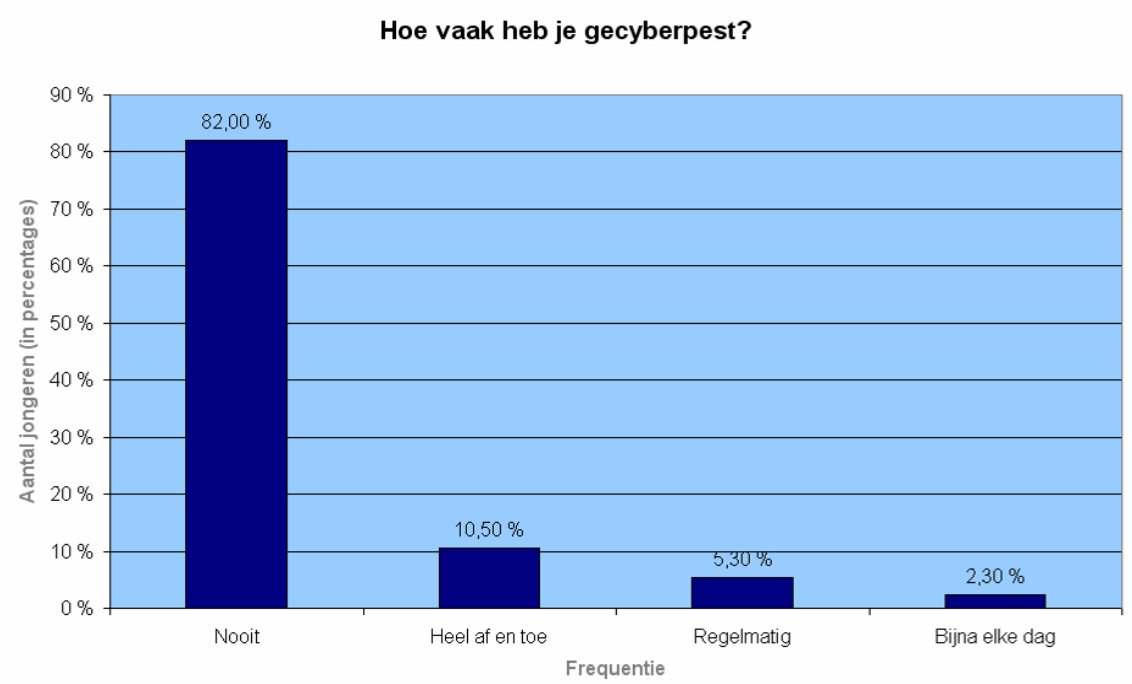
Tijdens het onderzoek kregen de jongeren niet alleen vragen voorgeschoteld die polsten of ze al eens het slachtoffer werden van cyberpesten, maar ook vragen of ze wel al eens iemand hadden gecyberpest. In onderstaande grafiek vindt u enkele vormen van cyberpesten terug met het daarbijhorende percentage jongeren dat zich reeds aan deze vorm van cyberpesten schuldig maakte.

De meest voorkomende vormen van cyberpesten staan vooraan in de grafiek, de minst voorkomende vormen van cyberpesten waarvan men dader was (bij de jongeren die ondervraagd werden) komen achteraan voor in de grafiek. Van meest voorkomend naar minst voorkomend dus.


Frequentieverdeling daders van verschillende vormen van cyberpesten
Aantal jongeren (percentages)
0 %
5 %
10 %
15 %
20 %
25 %
30 %
35 %
30,80 %
23,70 %
16,90 %
14,60 %
12,90 %
11,60 %
11,20 %
8,80 %
8,50 %
7,50 %
5,40 %
4,50 %
Iemand misleid door te doen alsof je iemand anders bent
Iemand beledigd of bedreigd via internet of GSM
Iemand uitgesloten uit een online groep
In iemands e-mailbox ingebroken en het paswoord veranderd
Roddels verspreid over iemand via internet of GSM
Op een website gestemd dat je een bepaalde persoon niet leuk vindt
Private of beschamende dingen over iemand verspreid via het internet
Ingebroken in de e-mailbox van een ander en berichten gestuurd naar zijn/haar contactpersonen
Enorm veel of grote berichten naar iemand gestuurd om zijn of haar computer te laten vastlopen
Opzettelijk een virus doorgestuurd
Dingen die iemand in vertrouwen had verteld, op een website geplaatst of doorgestuurd naar anderen via SMS of e-mail
Ingebroken in een computer en persoonlijke informatie gestolen
Vormen van cyberpesten

6.4.2.2 Frequentie van cyberpesten waarbij men dader was

In de vragenlijst bevroeg men de jongeren ook over hoe vaak ze in de afgelopen drie maanden gecyberpest hadden. In onderstaande grafiek vindt u de antwoorden.



6.4.2.3 Wie cyberpest men?

Aan de daders van cyberpesterijen vroeg men wie ze gecyberpest hadden. De jongeren konden meerdere antwoordmogelijkheden aanstippen, omdat men mogelijk meerdere slachtoffers gecyberpest had. Hieronder volgen de resultaten:

- 19,3 % cyberpestte één of meerdere personen die hij/zij enkel via het internet kent.
- 47,8 % cyberpestte één of meerdere onbekenden.
- 52,7 % cyberpestte één of meerdere personen die hij/zij ook in de echte wereld kent.

6.4.3 Verband tussen cyberpesten en geslacht

In Vlaanderen zijn er momenteel meer jongens die zich schuldig maken aan cyberpesten dan meisjes.

Volgens de resultaten van het onderzoek beweerden 72,9 % van de jongens nog "nooit" iemand anders te hebben gepest via internet of gsm, bij de meisjes was dit 85,3 %.

De oorzaak van dit verschil ligt waarschijnlijk in het feit dat Vlaamse meisjes door hun ouders meer beperkt worden in hun internetgebruik. Bij meisjes zijn de ouders ook meer betrokken bij hun internetgebruik.

6.4.4 Verband tussen cyberpesten en leeftijd

Cyberpesterijen nemen volgens onderzoek toe met de leeftijd, en nemen nadien weer af. De leeftijd waarbij het cyberpesten (zowel voor cyberslachtoffer als cyberdader) afneemt, ligt gemiddeld op twintig jaar.

De hoofdreden van dit verschil komt door de betrokkenheid van ouders bij het internetgebruik van hun kinderen. Naarmate de jongeren ouder worden, mogen ze langer op het internet vertoeven. De factoren die cyberpesten in de hand kunnen werken zoals het aantal minuten internet per week, de geavanceerde internetkennis, het aantal mensen die men enkel online kent, … stijgen met de leeftijd en nemen daarna weer af.

6.4.5 Verband tussen cyberpesten en studierichting

Uit onderzoek blijkt dat er een relatie bestaat tussen cyberpesten en de studierichting die men volgt. Leerlingen van het ASO hebben gemiddeld minder ervaring met cyberpesten dan leerlingen uit het BSO.

6.4.6 Verband tussen cyberpesten en ICT-gebruik

Onderzoek toont aan dat er een verband bestaat tussen cyberpesten en ICT-gebruik. Zo kunnen we stellen dat jongeren die veel tijd spenderen op het internet, die beschikken over geavanceerde internetkennis, die een grote internetafhankelijkheid hebben, die via het internet vaak praten met onbekenden en die vaak hun paswoorden aan 'vrienden' doorgeven, meer kans maken om slachtoffer of dader te worden van cyberpesten.

Opmerkelijk is wel dat cyberpesters minder betrokken en minder controlerende ouders hebben, en dat cyberslachtoffers een grotere voorkeur hebben om dingen via het internet te doen zoals bijvoorbeeld een ruzie uitpraten, persoonlijke informatie delen, …

6.4.7 Verband tussen cyberpesten en traditioneel pesten

In Vlaanderen blijkt er een sterke samenhang te zijn tussen de traditionele pesterijen en cyberpesterijen en dit vooral in de 'rollen' die men aanneemt. Is men slachtoffer van traditioneel pesten, dan is men vaak ook slachtoffer van cyberpesten. Is men een traditionele pester, dan is men vaak ook een cyberpester.

Het ziet er dus naar uit dat het traditionele pesten (vaak met behoud van rollen) wordt verdergezet via de nieuwe technologische middelen. Of we kunnen het ook omdraaien: cyberpesten kan ook aanleiding geven tot gewoon pesten.

6.5 Gevolgen van cyberpesten

Cyberpesten kan gedeeltelijk bekeken worden als een uitbreiding van het traditionele pesten. We kunnen dus aannemen dat een groot aantal gevolgen van traditioneel pesten ook gelden voor het cyberpesten. In sommige gevallen kan cyberpesten leiden tot minderwaardigheidscomplexen, afsluiting van de buitenwereld, in erge gevallen zelfs tot zelfdoding, …

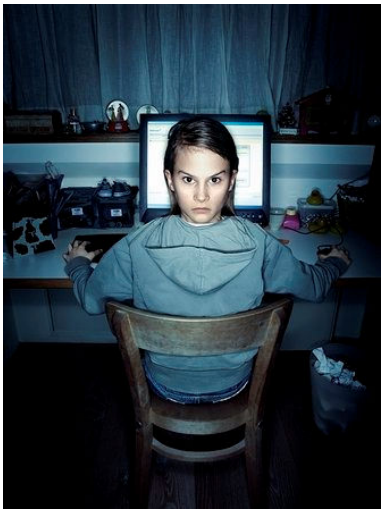
Het meest voorkomende gevolg van cyberpesten is depressiviteit. Vaak wordt deze depressiviteit in de hand gewerkt door de machteloosheid die het slachtoffer voelt en dit vooral door de reikwijdte en het anonieme karakter van cyberpesten. Zelfs in de thuisomgeving kan men gecyberpest worden en meestal weet men niet door wie omdat de cyberpester zijn echte identiteit verbergt.

Onderzoeker Baruch (2005) deed onderzoek naar het pesten via e-mail op het werk. Uit zijn onderzoek bleek dat pesten via e-mail in een werksituatie samenhing met negatieve attitudes van het slachtoffer ten opzichte van de job en de organisatie. Ten gevolge van deze pesterijen verlieten veel slachtoffers daarom hun huidige job.

6.6 Acties tegen cyberpesten

Net zoals er geen perfecte en sluitende oplossing is voor traditioneel pesten, zo is er ook geen kant-en-klare oplossing voor cyberpesten. Alles hangt ook af van de specifieke situatie, van het karakter van de cybergepeste, …

Toch kunnen we stellen dat het belangrijk is dat er maatregelen genomen worden om cyberpesten te voorkomen. Sensibilisering van jongeren, ouders en scholen is daarom een must.



Jongeren zouden bijvoorbeeld op school gesensibiliseerd kunnen worden en zo onder meer te weten komen wat cyberpesten precies is, dat het maatschappelijk niet aanvaardbaar is en dat het heel wat gevolgen kan hebben. Ook richtlijnen voor een veiliger cyberwereld zijn hierbij niet zinloos. Ook kan de aanpak van cyberpesten niet losstaan van een algemeen schoolbeleid inzake pesten op school.

Geef leerlingen vooral het gevoel dat ze hun cyberpestproblemen moeten melden en dat er dan samen naar een oplossing wordt gezocht. Het is natuurlijk belangrijk dat jongeren vertrouwen hebben in ouders en leerkrachten om problemen te melden. Ook de Kinder- en Jeugdtelefoon (KJT) is een plek waar kinderen op een anonieme manier hun verhaal kunnen doen, ook over cyberpesten. Een luisterend oor is voor slachtoffers vaak heel belangrijk.

Ook het voorlichten van ouders is niet onbelangrijk, omdat cyberpesten ook aanwezig is in het privéleven. U bent nergens meer veilig voor cyberpesterijen. Het is belangrijk dat ouders weten waarmee hun kinderen in de cyberwereld bezig zijn en dat ze er met hun kinderen over kunnen praten.

Verder wil ik aanstippen dat de samenwerking tussen ouders en de school (inclusief leerkrachten) enorm belangrijk is bij cyberpesten. Het slachtoffer is namelijk op geen enkele plek meer veilig voor zijn/haar cyberpesters.

Er bestaan al heel wat websites over cyberpesten, die over het algemeen volgende richtlijnen geven:

<u>Richtlijnen voor ouders</u>

- Plaats de computer op een goed zichtbare plek in het huis. Zo kunt u af en toe eens kijken wat uw kind aan het doen is op de computer en op het internet.
- Het is belangrijk dat u weet wat uw kind doet op het internet en wie zijn/haar online vrienden zijn.
- Geef uw kind waarden en normen mee in zijn/haar gedrag tegenover anderen, zodat het geen online pester wordt.
- Praat met uw kind(eren) over wat toelaatbaar is op het internet en wat niet.

<u>Richtlijnen voor potentiële slachtoffers</u>

- Geef via het internet zo weinig mogelijk persoonlijke informatie, foto's van uzelf, … door aan anderen en zeker niet aan mensen waarvan u hun echte identiteit niet kent.
- Vertel aan niemand uw paswoord(en).
- Geloof niet alles wat er op het internet te lezen valt en/of wat u er ziet.
- Gebruik nettiquette (gedragscode voor het gebruik van e-mail en internet).

- Stuur geen berichten naar iemand waar u boos op bent.
- Stuur geen berichten terug naar een cyberpester.
- Informeer uw internetprovider als u gepest wordt via internet.
- Bewaar e-mails en andere berichten van de cyberpester.

Richtlijnen voor scholen

- Informeer de leerkrachten, leerlingen en ouders over de ernst van cyberpesten.
- Voeg in het schoolreglement een clausule in om cyberpesten tegen te gaan en cyberpesters aan te pakken.
- Laat de leerkrachten ook cyberpesten opnemen in preventiemaatregelen zoals bijvoorbeeld het anti-pestcontract.

DEEL 2 DE VIRTUELE SECOND LIFE-WERELD

Second Life is op zich geen internetgevaar, daarom wordt dit in een afzonderlijk deel van mijn eindwerk opgenomen. Het voorlaatste hoofdstuk van dit deel besteedt aandacht aan de gevaren van Second Life.

Second Life is de nieuwe internethype van het moment. Sinds het ontwerpbureau Linden Lab Second Life in 2003 releasete, hoort u de naam meer en meer vallen. Ook in de professionele wereld heeft Second Life al heel wat bekendheid verworven. Ondanks zijn bekendheid wordt maar zelden een concrete uitleg gegeven over wat het is en wat u ermee kunt doen. In dit hoofdstuk wordt daarom een korte en algemene uitleg gegeven over Second Life en zijn eventuele gevaren. Een complete uitleg over Second Life en al zijn facetten is moeilijk te geven. Het is een 'wereld' die constant verandert en die virtueel enorme proporties begint aan te nemen.

1 Second Life in algemene termen

Letterlijk vertaald betekent Second Life een tweede leven. Maar wat is het nu precies? We kunnen Second Life definiëren als een digitale, driedimensionale online wereld. Sommigen zien het als een ontspannend, niets betekenend spel; anderen zien het als een tweede leven waarin ze (virtueel) al hun dromen en idealen grenzeloos kunnen nastreven. In Second Life bent u vrij om te doen en te laten wat u wilt. Er zijn weinig beperkingen in Second Life en daardoor gooien sommigen alle remmen los als ze zich in Second Life bevinden.

In Second Life heeft u de mogelijkheid om te zijn wie of wat u maar wilt, zonder dat de andere spelers (alias medebewoners) uw echte identiteit te weten komen. Wat u ook voor (erge) dingen doet in uw tweede leven (bijvoorbeeld mensen doodschieten, een sexclub openen, met 50 verschillende bewoners sex hebben, …), geen haan die er in het echte leven naar kraait.

Eén van de zaken waaraan Second Life zijn succes te danken heeft, is het feit dat u volledige vrijheid heeft om uw eigen leefwereld te ontwerpen. U kunt stellen dat bijna alles wat u in de wereld van Second Life ziet, ontworpen werd door Second Life-leden. Heeft u bijvoorbeeld een sofa nodig, dan kunt u een sofa kopen van een gebruiker die dit reeds aanmaakte, maar u kunt ook zelf een sofa maken die voldoet aan uw eigen wensen. Of het nu een sofa is, een huis, een winkel, kleren, … elk ontwerp ontstaat door 'prims'. Prims zijn gele kubussen die u naar eigen wensen kunt vervormen en die zo tot uw eigen ontwerp leiden. Als u creatief en inventief genoeg bent, kunt u zelfs uw eigen gemaakte voorwerpen verkopen en zo geld verdienen.

Naast uw eigen zaken ontwerpen, kunt u in Second Life nog heel wat meer zaken doen. U kunt er onder andere ook online mensen ontmoeten, met Second Life-vrienden praten, samen dingen doen, … U kunt het zo gek niet bedenken of u kunt het doen in de virtuele wereld van Second Life.

De gehele Second Life-wereld is onderverdeeld in gebieden. U heeft er bijvoorbeeld het gebied *Teen Second Life* dat enkel toegankelijk is voor Second Life-leden tussen dertien en zeventien jaar. Second Life-leden uit die leeftijdscategorie mogen niet in het hoofdgebied voor volwassenen komen en omgekeerd.

Elk gebied (of het nu voor jongeren of voor volwassenen is) bestaat uit een willekeurig aantal regio's, die onderling verbonden zijn en die land, water en lucht bevatten. Eén regio in Second Life bestaat uit vijfenzestigduizend vijfhonderdzesendertig Second Life-vierkante meters.

Volgende cijfers geven weer hoe succesvol Second Life is: de Second Life-wereld heeft (in juli 2007) reeds de kaap van acht miljoen inwoners bereikt waarvan er één miljoen zevenhonderdduizend de laatste zestig dagen inlogden. Logt u zich in, dan heeft u ongeveer elk moment twintigduizend à vijfentwintigduizend medebewoners die op dat moment ook online zijn. U kunt er zich wel alleen voelen, maar in feite bent u in die wereld nooit alleen… In België is Second Life nog niet zo'n groot succes als in andere landen, toch logden reeds vijftigduizend Belgen in in Second Life.

2 Uw avatar

In Second Life 'speelt' u met een avatar. Een avatar is een virtuele vertegenwoordiger van een Second Life-lid. U kunt een avatar ontwerpen die een kopie is van uzelf, u kunt een avatar met een dierenhuid ontwerpen of u kunt een extravagante onwereldse avatar ontwerpen. De bedoeling is dat u uw fantasie en creativiteit de vrije loop laat en deze regel geldt voor alles wat u in Second Life doet. Toch kiest het grootste deel van de Second Life-inwoners voor een menselijke avatar en vaak een die voldoet aan hun ideaalbeeld. Via uw avatar, kunt u er in de virtuele wereld uitzien zoals u er al altijd heeft willen uitzien (mits wat behendigheid en tijd).

Appearance, hier kan ik het uiterlijk en de kleren van mijn avatar aanpassen.

De naam van uw avatar kunt u in Second Life niet veranderen (de voornaam voor uw avatar mag u zelf kiezen, voor de familienaam heeft u keuze uit een uitgebreide lijst). U kunt het uiterlijk van uw avatar zo vaak veranderen als u wilt. Het ene uur kan uw avatar een man zijn, het andere uur kan het een vrouw zijn en de dag erop kan uw avatar er als een marsmannetje uitzien. Sommige leden baseren zelfs hun avatars op fictieve figuren uit echte films, stripverhalen of boeken (dieren, vampieren, helden, …).

De keuze van uw avatar heeft geen invloed op de toegang, opties en rechten in Second Life, behalve als zij natuurlijk de normen en waarden van de samenleving schenden. Als een jongere bijvoorbeeld een provocerende en gruwelijke avatar ontwerpt, bestaat de kans dat hij/zij met die avatar geen toegang tot Second Life krijgt. Maar u kunt zich natuurlijk afvragen waar de grens ligt die bepaalt wat die normen en waarden precies zijn. Hou er wel rekening mee dat uw avatar veel zegt over wie u bent. De keuze van uw avatar weer-

spiegelt (meestal) uw persoonlijkheid en mentaliteit. Voor andere Second Life-bewoners is uw avatar wie u bent, hou dat steeds in gedachten.

3 Second Life-geld

U kunt heel wat virtuele zaken ontwerpen in Second Life, maar u kunt er natuurlijk ook heel wat virtuele zaken kopen zoals bijvoorbeeld kleren, vliegtuigen, juwelen, … zelfs geslachtsdelen staan in de aanbieding. Net zoals in het echte leven heeft u geld nodig om iets te kopen. Daar hebben de ontwerpers van Second Life natuurlijk ook aan gedacht en ze hebben een eigen valuta ontworpen: de Linden-dollar (afkorting: L$).

Hoe komt u nu aan Linden-dollars? Er zijn hiervoor verschillende manieren. U kunt er onder andere voor kiezen om een virtuele baan aan te nemen (dit kunt u bijvoorbeeld doen via de Second Life-classifieds [advertentiepagina's]). U kunt bijvoorbeeld ook een eigen virtueel bedrijf opstarten en op die manier proberen winst te maken, u kunt voorwerpen ontwerpen die u dan verkoopt aan anderen, u kunt geld verdienen door te gokken, … Heeft u echt geen zin om u uit te sloven voor enkele Linden-dollars dan kunt u zelf een tijdje gaan zitten in een soort kampeerstoel of een dansje wagen op de dansvloer, waarvoor u in ruil enkele Linden-dollars ontvangt. En geloof het of niet, af en toe kunt u zelfs de Linden-dollars gewoon van de bomen plukken.

Mijn avatar in een kampeerstoel, dit is een manier om geld te verdienen als u heel veel geduld heeft. Zo krijg ik om vijftien minuten in de kampeerstoel te zitten drie Linden-dollars.

U kunt het zo gek niet bedenken of het is 'realiteit' in Second Life. U kunt er zelfs echte dollars tegen Linden-dollars omwisselen en omgekeerd. Dit omwisselen gebeurt via enkele valutadiensten van derden zoals bijvoorbeeld bij Linde X. Als we praten over geld omwisselen, dan heeft u natuurlijk een wisselkoers nodig. Een wisselkoers wordt gekenmerkt door zijn schommelend karakter en dit is hier niet anders (bijvoorbeeld afhankelijk van het aantal betalende accounts, van de Linden-dollars in omloop, …). Op dit moment (in 2007) kunnen we stellen dat 1 USD (± 0,73 EUR) ongeveer 275 Linden-dollars waard is. Gelukkig heeft de Linden-dollar van Second Life veel meer koopkracht dan echt geld.

Maar wees gerust, in Second Life kunt u ook heel wat zaken gratis krijgen of voor een symbolisch bedrag van één Linden-dollar .

4 Wat te doen met uw nieuwe leven

Wanneer u met uw avatar voor de eerste keer inlogt in Second Life, belandt u op Orientation Island waar u kort uw eerste stapjes als virtueel personage leert zetten. De tweede stop van uw verblijf is op het eiland Help Island, waar u stapsgewijze uitleg krijgt over hoe te leven in Second Life. Daarnaast vindt u op het eiland ook gratis spullen (in Second Life freebies genaamd) zoals bijvoorbeeld kleren, juwelen, meubels, … U heeft er ook demonstratiegebieden waar u heel wat bijleert en op het eiland vindt u ook mentors die met plezier uw eventuele vragen beantwoorden. Het is goed om een tijdje te blijven op Help Island zodat u het werken met uw avatar wat onder de knie krijgt. Maar vergeet niet dat dit maar een verkenningseiland is. Er zijn veel mensen die afhaken op Help Island omdat ze denken dat Second Life enkel dit is.

Na uw bezoek aan deze twee eilanden kunt u zichzelf teleporteren (verplaatsen), door middel van coördinaten of door aanduiding op een kaart, naar het vasteland van Second Life. Dit is een definitieve stap, want met dezelfde avatar kunt u niet meer terug naar Orientation Island en Help Island. Wilt u toch nog wat bijleren over Second Life of zelfs een cursus krijgen over een bepaald onderwerp die u in het echte leven kunt gebruiken (bijvoorbeeld over de betekenis van de verkeersborden), dan kunt u altijd terecht bij de vele scholen en universiteiten die u in Second Life kunt vinden.

Als u wat geëxperimenteerd heeft met Second Life, dan kunt u zich gaan afvragen wat u nu precies moet aanvangen met uw nieuwe leven. In principe is er geen vijand die u moet verslaan of is er geen geldbedrag dat u moet bereiken. Second Life heeft als hoofddoel mensen te amuseren en voor heel veel Second Life-bewoners vormt de virtuele wereld gewoon een mooie plek om andere mensen van over de hele wereld te ontmoeten. Uw avatar kan bijvoorbeeld contact zoeken met een andere avatar en er een gesprek mee aangaan en/of samen gaan zwemmen, naar een café gaan, gaan bowlen, kunstgalerijen bezoeken, … U kunt zich zelfs aansluiten bij een groep die dezelfde interesses als u delen. Zo heeft u in Second Life bijvoorbeeld een Nederlandse groep waarvan het 'hoofdkwartier' een eiland is waar een gezellig Nederlands marktje en een typische Nederlandse boerderij werden nagebouwd.

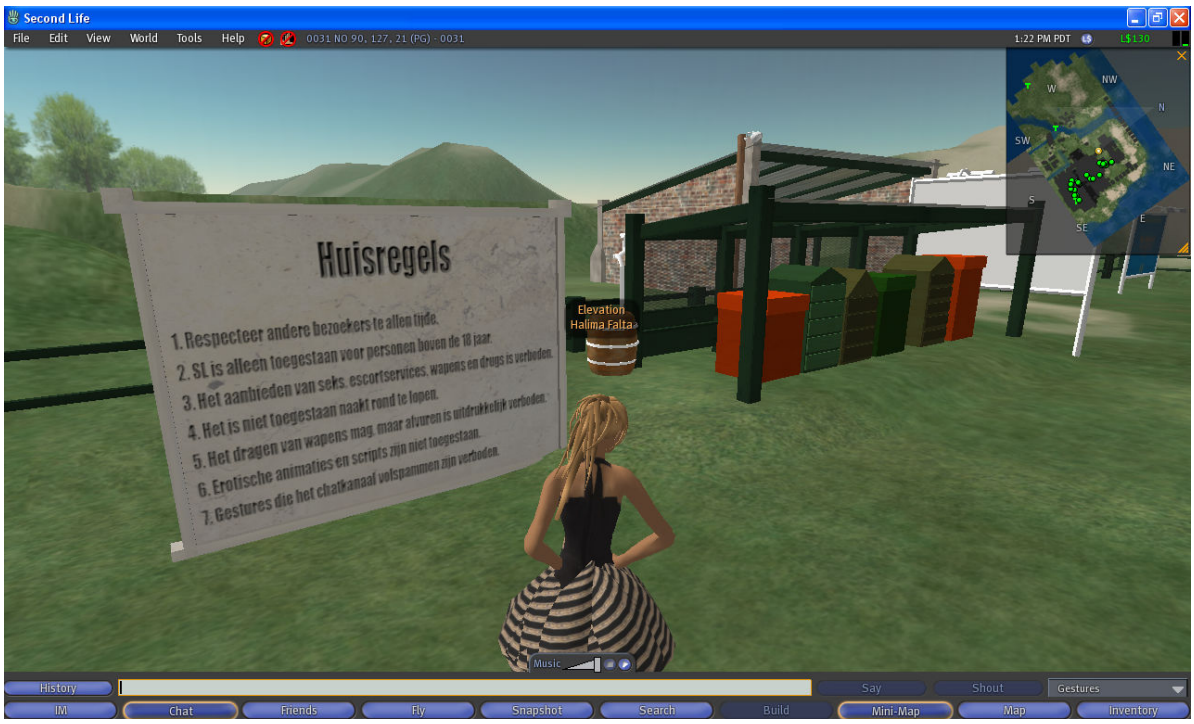
Voor veel bewoners vormt Second Life een ideale plek om hun talenten als uitvinder en/of kunstenaar te ontwikkelen. U kunt er voorwerpen ontwerpen, huizen bouwen, fotograferen, films met avatars maken, … Als u een film maakt, kunt u zelfs geselecteerd worden als kanshebber voor een Second Life-filmfestival, waar u een prijs kunt wegkapen van honderdduizend Linden-dollar (± 265,43 EUR). Second Life heeft zelfs een eigen programmeertaal - Linden Scripting Language (LSL) genaamd -waarmee u zaken kunt verfijnen door er bijvoorbeeld bewegingen aan toe te voegen.

'Mijn avatar' is iets aan het bouwen, creatief met prims, de gele kubussen die de basis zijn voor zowat alles wat in Second Life bestaat. Aan de rechterkant van mijn prim staat een bed dat gemaakt werd door een Nederlandse medebewoner. Indien ze dat wenst, kan ze dit bed verkopen aan anderen voor een aardig aantal Linden-dollars.

U kunt zelfs echt rijk worden door Second Life te spelen. Zakenvrouw Anshe Chung is daar een mooi voorbeeld van. Zij is een grootgrondbezitter in Second Life en doet er net zoals in het echte leven vastgoedzaken. Haar jaarlijkse Second Life-inkomen is geraamd op 109 489,05 EUR . Door de mogelijkheden van Second Life is Ansche Chung voorlopig niet meer weg te slaan van het lijstje van de rijkste en beroemdste mensen van de wereld. Toch moeten we niet te hard van stapel lopen want Second Life-miljonairs zijn uitzonderlijk. U moet al ontzettend veel tijd en creativiteit in Second Life stoppen om er een flinke duit aan over te houden. Maar het is werkelijkheid, sommigen kunnen maandelijks van een extraatje genieten door hun Second Life-inkomsten te laten wisselen in Amerikaanse Dollar. Wie niet waagt, niet wint…

Second Life wordt tegenwoordig niet alleen meer gebruikt om plezier te beleven, maar het wordt ook meer en meer een ontmoetingsplaats waar wetenschappers, onderwijzers, studenten, … samenkomen. Of die nu om de hoek wonen of duizenden kilometers van elkaar, in Second Life vormt dit geen enkel probleem. Het verschil tussen het traditionele chatten en het chatten in Second Life is dat u bij het chatten in Second Life iemand fysiek voor u ziet staan, ook al is dit maar een avatar.

Gezien u in Second Life heel veel vrijheid heeft, mag u toch niet overal alles doen wat u maar wilt. Zoals eerder vermeld, bestaat Second Life uit regio's en die regio's worden bestuurd door middel van regels die van regio tot regio kunnen verschillen. In sommige regio's, die eigendom zijn van een bepaalde avatar of van een groep avatars, mag u bijvoorbeeld niet vliegen (DE manier van verplaatsen in Second Life), mag u niet naakt rondlopen of mag u niet schieten, … Maar wees gerust, er is genoeg grond te vinden die privé-eigendom is van een individu of van een groep waarvan de eigenaars alles toestaan. U kunt ook zelf privé-grond kopen – hiervoor heeft u wel een Premium-lidmaatschap nodig (zie verder) - en er uw eigen regels bepalen. Let wel op want vanaf meer dan vijfhonderdentwaalf vierkante meter moet u maandelijks kosten betalen voor grondgebruik; hoe meer vierkante meter, hoe meer u moet betalen.



Hier ziet u dat mijn avatar de huisregels leest van de Nederlandse regio in Second Life.

Het is nu eenmaal realiteit: virtuele seks is één van de populairste activiteiten in Second Life. Er zijn veel plaatsen waar gratis seks wordt aangeboden, maar uw avatar kan bijvoorbeeld ook naar een betalende seksclub gaan. Soms wordt u door een avatar uitgenodigd om samen iets leuks te gaan doen (winkelen, dansen, …) maar komt u in feite terecht in een sekskamer. Maar wat er ook plaatsvindt in Second Life, het vindt plaats met wederzijdse toestemming: iedereen die niet leuk vindt wat er gaande is, kan de wereld met één muisklik verlaten of kan zichzelf teleporteren.

5 Normen en waarden in Second Life

In de gemeenschap van Second Life gelden normen en waarden. Die normen en waarden staan op de notecard (een tekstbestand) 'Community Standards', die u kunt terugvinden in de Library (in de map Notecards). Die normen en waarden komen er in feite op neer dat u het plezier van andere bewoners niet moet vergallen. Gebruik net zoals in het echte leven uw gezond verstand om te bepalen wat aanvaardbaar is en wat niet. De notecard 'Community Standards' geeft zes hoofdzonden weer die onaanvaardbaar zijn in Second Life. U stemt hiermee automatisch in wanneer u een Second Life-lidmaatschap aangaat. Indien u toch over de schreef gaat, riskeert u een schorsing of zelfs een verbanning uit Second Life.

Er zijn zes hoofdzondes ('de grote zes' genaamd):

- Onverdraagzaamheid.
  Net als in het echte leven worden vernederende of minachtende opmerkingen over ras, godsdienst, geslacht of seksuele geaardheid niet toegestaan.
- Pesten.
  In de virtuele wereld kan pesten verschillende vormen aannemen, maar ze hebben één ding gemeen: ze ergeren en kwetsen iemand. Als u merkt dat uw daden of woorden iemand irriteren, moet u ermee ophouden.
- Daadwerkelijke bedreiging.
  Hieronder verstaat men het wegduwen of beschieten van een avatar in een gebied dat als veilig wordt aangegeven (u kunt dit zien als de status 'Safe' weergegeven wordt als een pictogram op de bovenste informatiebalk). Ook andere avatars het leven zuur ma-

ken door hen met gescripte objecten te bestoken (bijvoorbeeld met een mes), is verboden.

- Openbaarheid.
  U kunt informatie over een bepaalde bewoner delen met anderen indien deze informatie in het profiel staat van de betrokken bewoner of als hij/zij zijn/haar toestemming heeft gegeven om die bepaalde informatie te delen.
- Onfatsoen.
  Als u bepaalde zaken doet die andere bewoners kunnen choqueren, doe het dan op privé-grond die dit toestaat en doe dit zeker in gebieden die alleen toegankelijk zijn voor volwassenen.
- De rust verstoren.
  Iedere bewoner heeft recht op een plezierig en rustig bestaan in Second Life. Iemand lastigvallen en irriteren is niet de bedoeling van Second Life.

6 Soorten lidmaatschappen

Voorlopig heeft u in Second Life nog maar twee soorten lidmaatschappen: het Basic-lidmaatschap en het Premium-lidmaatschap.

Met het Basic-lidmaatschap heeft u gratis toegang tot Second Life. U kunt er genieten van alle activiteiten en privileges maar eigen virtuele grond kunt u met het Basic-lidmaatschap niet bemachtigen. Als u meer dan één Basic-account wilt (om bijvoorbeeld meerdere avatars te hebben), dan moet u voor elke extra Basic-account 9,95 echte Amerikaanse dollar betalen (± 7,26 EUR).

Wilt u een Premium-lidmaatschap, dan moet u maandelijks een bepaald bedrag betalen. Dit bedrag bedraagt gemiddeld 6,00 USD (± 4,38 EUR) per maand en is onder andere afhankelijk van de betalingswijze, het al dat niet spreiden van de betaling, … De bedragen zijn natuurlijk niet vast en kunnen dus ten allen tijde gewijzigd worden. Het grootste verschil tussen een Premium-account en een Basic-account is dat u met een Premium-account eigen Second Life-grond kunt kopen, waarop u bijvoorbeeld uw avatar kan laten wonen in een huis dat u zelf ontwerpt. Afhankelijk van hoe u betaalt, krijgt u naast de grondeigendomsrechten, een inschrijfbonus van duizend Linden-dollars en een wekelijkse toelage van vierhonderd Linden-dollars.

7 De toekomst van Second Life

Sommigen zijn van mening dat men Second Life niet echt een spel kan noemen omdat u er geen vast omschreven doelen moet bereiken en er geen score is die aangeeft of men al dan niet goed bezig is. Misschien denkt men dan ook dat Second Life geen lang leven beschoren is. Niets is minder waar, want voor veel bewoners is het een tweede leven waarin hun fantasieën en ontwerpen 'verwezenlijkt' kunnen worden. Dit is voor hen vaak meer waard dan een bepaalde score. Second Life wordt soms genoemd als de volgende generatie van het internet, al vind ik dat wat ver gegrepen. Toch blijkt Second Life belangrijker te worden. Dit blijkt uit onderstaande voorbeelden.

Winkelen is één van de meest favoriete bezigheden van de Second Life-bewoners. Pientere zakenlui hebben dit natuurlijk door en spelen daar gretig op in. U kunt bijvoorbeeld vanuit Second Life winkelen op Amazon.com. Nee, niet de mensen die Second Life ontwierpen, hebben dit bedacht en deze virtuele 'winkel' ontworpen, maar de mensen van Amazon.com hebben dit bedacht en gerealiseerd.

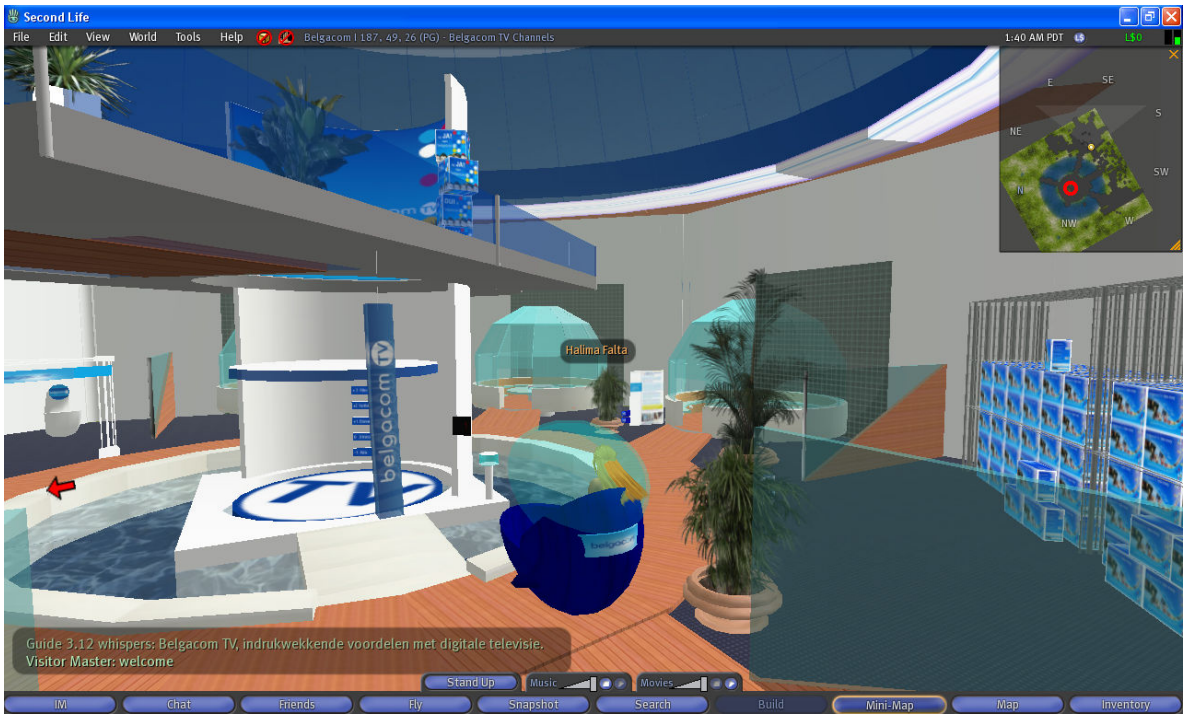
U kunt in Second Life bepaalde virtuele kleren kopen die u in echte boetieks ook kunt vinden. Zo heeft het kledingmerk American Apparel een virtuele winkel in Second Life geo-

pend, waarin ze virtuele versies van hun kleding verkopen en bij uw aankoop krijgt u een kortingbon voor de aankoop van dat artikel in het echt. Slim bedacht, vindt u niet?

Daarnaast is ook het bekende 20th Century Fox in de Second Life-wereld gestapt. Tijdens de première van de film 'X-Men: The Last Stand' op het Cannes filmfestival, lieten zij tegelijkertijd ook stukken van deze film zien in Second Life.

Ook de Belgische en Nederlandse bedrijfswereld vinden hun weg naar Second Life. Zo kunt u er bijvoorbeeld de locatie van het Nederlandse Randstad bezoeken, waar u een virtuele job kunt vinden (om zo Linden-dollars te verdienen) en u kunt er zelfs vacatures vinden voor echte (real-life) jobs; ook sollicitatiegesprekken worden er soms gevoerd. Ook het Belgische Belgacom heeft sinds kort zijn eigen locatie in Second Life. Interessant om weten is dat u er een geautomatiseerde tour kunt doen en op die manier uitleg krijgt over wat het Belgacom-eiland zoal te bieden heeft. U kunt er onder andere leren hoe u een draadloze modem moet installeren, u vindt er informatie terug over de Proximus-diensten, informatie over de digitale televisie, … U kunt er uw avatar zelfs even laten relaxen terwijl hij/zij (en u als gebruiker natuurlijk ook) een Popey-tekenfilmpje bekijkt.

Een schermafdruk uit de locatie van Randstad. Hier ziet u twee borden die u kunt aanraken. Zo ziet u open vacatures van virtuele jobs of van 'echte' jobs. Gek genoeg kunt u ook hier voor echte jobs een virtueel sollicitatiegesprek voeren.



Hier ziet u mijn avatar op het Belgacom-eiland. Ze zit in een soort vliegende bol waarmee ze een rondleiding krijgt over wat het eiland zoal te bieden heeft: een plek waar u informatie vindt over Belgacom TV, Proximus-diensten, …

Bedrijven zien Second Life als een soort website, een plaats waar ze hun producten kunnen voorstellen. Als een bedrijf meegaat in de 'stroom' van Second Life, dan ervaren de meeste gebruikers dit als een modern en vernieuwend bedrijf dat moeite doet voor zijn klanten en zijn publiciteit. De bedoeling van die bedrijven is natuurlijk om meer naambekendheid te krijgen en meer succes te boeken.

Men wil Second Life ook gebruiken als een platform voor het onderwijs. Tegenwoordig zijn scholen, universiteiten, leerkrachten en studenten aan het experimenteren om Second Life te integreren in het onderwijs. Zo zijn er bijvoorbeeld al enkele universiteiten die een ruimte inrichten zodat afgestudeerde studenten van een bepaalde universiteit elkaar kunnen ontmoeten en informatie met elkaar kunnen uitwisselen. Er is zelfs een Second Life-bewoonster die aan de hand van authentieke kaarten enkele Egyptische tempels, die vroeger echt hebben bestaan, virtueel nabouwt. Dergelijke zaken zijn bijvoorbeeld handige hulpmiddelen voor het secundair onderwijs.

8 Enkele ervaringen van Second Life-bewoners[1]

Of u nu een Second Life-bewoner bent of niet, u vraagt zich soms af wat andere gebruikers aanvatten met hun tweede virtuele wereld en hoe zij denken over Second Life. In het officiële handboek van Second Life doen enkele anciens hun verhaal. Natuurlijk moeten die verhalen met een korreltje zout genomen worden, want verhalen over mensen die minder goede ervaringen hebben met Second Life vindt u in het boek niet. Waarschijnlijk zijn de verhalen van succesvolle oude rotten in het 'vak'. Hieronder vindt u een greep uit het assor-

[1] Rymaszweski, M., JAMES AU, W., WALLACE, M., WINTERS, C., ONDREJKA, C., BATSTONE-CUNNINGHAM, B., ROSEDALE, P., *Second Life: het officiële handboek*, Omega, Diemen, 2007, 342 pagina's

timent van verhalen die u misschien nog wat over Second Life zullen bijleren. Zoals eerder al gezegd, is het haast onmogelijk alles over Second Life te weten of te vertellen.

Enkele foto's uit Second Life geven u een idee van wat u in de virtuele wereld zoal kunt vinden.

Llianexsi Sojourner

"Zelf hou ik om vele redenen van Second Life… deze wereld biedt kansen aan iedereen. Ik hou ervan omdat ik ervan geniet zo veel dingen te kunnen doen die in het echt niet mogelijk zijn… en omdat ik het geweldig vind de middelen te hebben om alles uit mijn fantasie werkelijkheid te laten worden. Ik geniet ervan om mensen te ontmoeten die ik in het echt nooit had kunnen ontmoeten.

En ja, ik geniet van Second Life omdat ik ervan houd er zo goed uit te kunnen zien als ik wil, om in een handomdraai mijn uiterlijk te kunnen veranderen en om er totaal afwijkend van mijn echte uiterlijk uit te kunnen zien.

En ik begrijp het veiligheidsidee volledig… het is geweldig om hier de controle te hebben, om me geen zorgen te hoeven maken over mijn eigen veiligheid. Dat geldt hier net zo voor mannen als voor vrouwen, maar ik denk dat het vooral voor vrouwen van belang is."

Michael Control

"Ik heb altijd Jan-met-de-pet willen zijn. Ik ben een schrijver van beroep in het echte leven en schrijvers zijn nu eenmaal geen alledaagse mensen, daarom zijn en blijven het ook schrijvers. En als je, net zoals ik, er opvallend uitziet (en niet noodzakelijkerwijs in positieve zin) dan kan de behoefte om in de massa op te gaan obsessieve vormen aannemen.

Second Life heeft mij die mogelijkheid gegeven: een kant-en-klare, goed uitziende avatar, waarvan er dertien in een dozijn gaan. Ik heb wel een paar aanpassingen aangebracht, vooral omdat ik heel wat tijd gestoken heb in het spelen met de tools om het uiterlijk van de avatar aan te passen. Les één, als je meneer Incognito in Second Life wilt zijn, gebruik je de standaard-avatar met een paar kleine wijzigingen. Als je helemaal geen veranderingen maakt, val je op, zo van 'Wie is die nieuweling die er nog niet achter is dat je het uiterlijk van je avatar kunt veranderen?'

Hoewel ik de voordelen van het Premium-lidmaatschap had, dankzij de genereuze lui van het Linden Lab, wilde ik Second Life ervaren zoals een schipbreukeling een onbewoond eiland ervaart: geen hulp van de buitenwereld in de vorm van giften en ook niets kopen. Alles wat ik droeg of bezat zou door mij zelf gemaakt moeten worden. In verband daarmee heb ik zo'n beetje alle handleidingen uit mijn hoofd geleerd en ging ik tijdelijk in een lege 'zandbank' (bouwgrond) zitten. Na een paar uur was ik in staat om snel eenvoudige objecten te bouwen met simpele animaties (zonder wroeging kopieerde ik de

bestaande scripts in plaats van dat ik ze zelf vanaf het begin ontwierp). Ik was er echt trots op en toen verscheen er een vrouw, een erg mooie vrouw met een paar vleugels, waar de meeste engelen jaloers op zouden zijn. Binnen ongeveer vijf minuten bouwde ze een prachtig tweepersoonsbed, compleet met een uitgebreid versierd hoofd- en voeteinde. Ze nodigde me niet uit om het te proberen en ik maakte me stilletjes uit de voeten en ik voelde me heel klein. Dit betekende het dus om Jan-met-de-pet te zijn! Niet zo leuk als je op zoek bent naar een beetje actie.

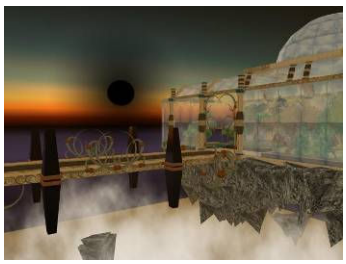
Gelukkig leidde dit incident er wel toe dat ik iets ontdekte wat ik aanvankelijk over het hoofd had gezien in het begin van mijn virtuele leven: je hoeft niet iets te doen waar je geen zin in heeft. Je kunt zo'n beetje alles wat je hartje begeert gratis krijgen, of in ieder geval voor een Linden-dollar. De enige uitzondering is wanneer je een eigen virtuele plek wilt hebben, of je nu koopt of huurt. Persoonlijk had ik daar geen behoefte aan, wat mij betreft is één van de opwindendste dingen van Second Life, dat je niet die dingen nodig heeft die je in het echte leven wel nodig heeft. Je heeft geen huis nodig en het regent nooit; sterker nog: je kunt zelfs de zon laten schijnen zoals je zelf wilt."

<u>Frank Freelunch</u>

"Ik had één voordeel: een man, Michael Control, deelde zijn kennis met mij voordat ik ook maar een stap in Second Life zette. Eén van de dingen die hij me vertelde was dat iedereen er zóóóóó goed uitzag dat het haast pijn deed om er naar te kijken.

Overigens wilde ik zelf geen 'stuk' zijn; ik koos voor een andere richting. Een beetje dollen met de tools om het uiterlijk van de avatar aan te passen en klaar was Kees! Ik was een vriendelijke bouwvakker in de bar waar ze goedkoop bier verkopen. Het standaard witte T-shirt, jeans, bierbuik, geschoren hoofd; ik trok er nog een vriendelijk, maar beetje dromerig gezicht bij voor een nog beter effect. Eerste waarneming: ik was de enige lelijke man in de hele virtuele wereld. Daar viel ik mee op! Maar andere mensen snapten het niet en wanneer ik met iemand praatte hing de vraag in de lucht: 'Je ziet er in het echte leven zeker ook zo uit?'

Omdat ik een bouwvakker was, besloot ik wat te gaan bouwen. Ik kreeg mijn eerste First Land-kavel en begon een huis te bouwen. Eerst moest het land vlak gemaakt worden, je weet dat dit niet gemakkelijk is. Ik vermoed dat dit ook de reden is dat je zoveel kavels te koop ziet die aangeboden worden als vlakke en groene grond en vele malen meer kosten dan de oorspronkelijke prijs. Wat je moet doen is eerst een klein gebied helemaal vlak maken en het naar jouw wensen zien op te hogen. Toen ik eenmaal mijn kavel op orde had, was het gemakkelijk om van daaruit verder te werken. Toen ik zo'n beetje op de helft was ging ik een pilsje pakken in Second Life, dat kan en je kunt zelfs een koelkast krijgen, zodat het lekker koel blijft. Toen ik terugkwam op mijn werk



viel me ineens iets op. Ik keek omhoog en daar was dat prachtige huis dat er eerst niet was, zo'n dertig meter zwevend boven de naastliggende kavel. Dus ik mompelde maar wat in mezelf en ik ging maar weer een biertje halen.

Mijn favoriete activiteit in Second Life? Games. Ik raakte verslaafd aan de Space Invaders op Help Island, in de echte wereld was ik er als kind al heel goed in. Dus toen ik eenmaal klaar was met bouwen, ging ik naar de speelhallen voor een beetje ontspanning. Voor de meeste games moet je betalen om ze te kunnen spelen, maar bijna alle game-plaatsen hebben kampeerstoelen en geldbomen. Je speelt een tijdje en als je geld op is, ga je even uitrusten op één van die betalende stoelen, misschien kun je, als je geluk heeft, zelfs geld van de geldbomen plukken. (Er zijn geldboom-plunderaars die van boom tot boom gaan om gratis geld te plukken en meestal zijn de bomen volledig kaal geplukt.)

Ik vind het leuk om rond te kijken en dus dwaalde ik veel rond en bezocht verschillende plaatsen. De plaats die ik het leukste vond? Dat zal je verbazen. Het was niet een exotisch eiland of een Japans dorp; het was het gedeelte van het vasteland wat ze Grignano noemen. Ze hebben daar een taxiservice en ik voelde me pas thuis in de virtuele wereld toen ik, nadat ik bij de taxistop had moeten wachten, een taxi nam. Je zou eigenlijk moeten lopen, rijden of een taxi nemen in SL in plaats van te vliegen of je te laten teleporteren, dan wordt de ervaring veel echter."

<u>Desmond Shang</u>

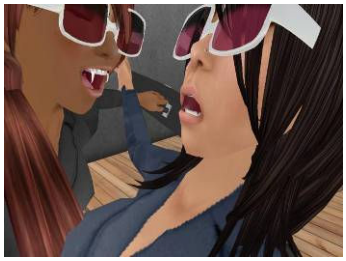
"Mijn Second Life-ervaring is nogal verbazingwekkend, echt waar. Ik maak normale, oude, gewone dingen die je over het algemeen in de 19de eeuw tegenkomt, gewoon voor de lol. Van alles, van lampen tot Victoriaanse huizen.

Op de één of andere manier zijn dit soort dingen nu eenmaal populair. Ik had dat nooit verwacht. Het kan zijn dat de 'alles mag-cultuur' die voortkomt uit de online-ervaring, velen snel de keel uit gaat hangen.

En dus, liever dan geld bij Second Life te verdienen, kocht ik een eiland, gewoon voor de lol. Misschien zijn er wel drie of vier mensen die ervan genieten om in een 19de eeuws dorpje aan de zee te leven om zodoende de kosten te drukken? Ik maakte een kleine Schotse vlag, opende het eiland Caledon en het dorp liep snel vol. Ineens was er een wachtlijst van ongeveer 50 personen.

Zo'n respons had ik niet verwacht. Ik denk dat je niets meer hoeft te doen dan wat land te kopen om mensen blij te kunnen maken. Het hele gebeuren leek op het aansteken van vuurwerk.

De gemeenschap ging zonder mij vanzelf verder. Binnen korte tijd waren er huizen en winkels, theekransjes, formele feesten en een ongelofelijk gevoel van plezier en de groei duurde



voort. Het gevoel om onderdeel te zijn van iets wat zowel wonderlijk als groter is dan jezelf, schijnt op iedereen invloed te hebben.

Ik sta ervan te kijken wat de gemeenschap bereikt heeft. We hebben een tram, gemaakt door een paar talentvolle bewoners, die een soort oriëntatiepunt is geworden. Bovendien zamelde de gemeenschap duizenden echte dollars in voor de American Cancer Society tijdens één van hun Relay for Life-campagnes. Het is een eer om ze allemaal te kennen.

Mijn dagelijkse bezigheden lijken nog het meest op die van een klusjesman. Ik zorg ervoor dat Caledon redelijk schoon is, repareer een aantal dingen die gemaakt moeten worden en ik beantwoord vragen. Er zijn ook heel wat vragen van de antiekkopers bij West Trade Imports Ltd. Zo nu en dan voeg ik wat land toe, wat natuurlijk altijd leuk is. Het gaat allemaal geruisloos; ik heb nog geen vervelende ervaring gehad met welke bewoners in Caledon dan ook.

Het is zeer waarschijnlijk dat, als ik het in het begin anders had aangepakt, de zaken er nu heel anders voor zouden staan. Dit is nu zo'n perfect voorbeeld van hoe een kleine beslissing later grote consequenties heeft. Ik moet toegeven, dat Second Life me zoveel meer heeft gegeven dan ik ooit had verwacht."

9 De gevaren van Second Life

We kunnen er niet onderuit, ook in Second Life ligt het gevaar op de loer. Misschien voelen sommige mensen zich veilig in Second Life, maar dit is eigenlijk onterecht en een beetje naïef. Natuurlijk wordt u niet constant belaagd, maar deze virtuele wereld begint meer en meer bekend te worden en dan gaan natuurlijk ook de cybercriminelen aan de slag. Hieronder worden enkele gevaren beschreven die sommige Second Life-bewoners al hebben ervaren.

Zoals reeds vermeld, vinden steeds meer criminelen en hackers hun weg naar Second Life. Ze maken een avatar aan en zoeken contact met andere bewoners. Ze lijken erg behulpzaam, want ze bieden u bijvoorbeeld nieuwe kleren aan die u al dan niet kunt accepteren. Maar wees alert, in deze giftbox zit misschien wel spyware die u heel wat last kan bezorgen. Via die spyware kan de dader heel wat informatie over u te weten komen zoals bijvoorbeeld uw accountinformatie, paswoorden,… Voor u het weet worden al uw virtuele bezittingen uit Second Life gestolen en worden ze verkocht voor echt geld op veilingsites zoals eBay.
Nogmaals… u kunt het zo gek niet bedenken: vanaf twaalf juli kunt u zich zelfs verzekeren bij het Nederlandse Univé tegen diefstal en schade in Second Life. U betaalt voor deze dienst halfjaarlijks tweehonderd Linden-dollar (± 0,53 EUR) en per schadeclaim kunt u maximaal tienduizend Linden-dollar (± 26,54 EUR) ontvangen.

Wanneer u in Second Life vertoeft, slaat u al snel een praatje met andere bewoners en die vragen u vaak om samen met hen mee te gaan en iets leuks te doen zoals samen gaan winkelen, op de kermis zitten, iets gaan drinken, … Vaak stemt u hier mee in omdat u wel iets leuks wilt doen in Second Life. Wanneer die avatar u meeneemt (teleporteert) naar een andere bestemming, dan is die vaak niet de onschuldige plaats waar u dacht terecht te komen. Vaak teleporteert hij/zij u naar een seksclub of een rustig, romantisch plaatsje dat hij/zij huurt voor zijn/haar seksuele bezigheden.
Ook steeds meer pedofielen krijgen deze mogelijkheid onder de knie en zoeken in Second Life kinderen op die ze via een omweggetje veroveren. Uit Nederlands onderzoek blijkt dat mannen, die virtuele betrekkingen hebben met kinderen, ook daadwerkelijk makkelijk overgaan tot echte seksuele handelingen met kinderen. Toch is iemand, die in België in een virtuele internetwereld verboden seksuele handelingen heeft met virtuele kinderen, voorlopig nog niet strafbaar. Mocht men een dergelijke maatregel invoeren, dan zou dit internationaal moeten gebeuren. Want waar trekt u de lijn voor Belgen in Second Life? Het wordt afwachten of er effectief zal ingegrepen worden.

Schrik niet, Second Life wordt ook gebruikt om iemand te pesten in het echte leven. Sommigen bouwen een avatar na die als twee druppels water lijkt op een kennis van hen die zij willen pesten. Ze laten die avatar dan bepaalde handelingen uitvoeren zoals seks hebben met een avatar die lijkt op de leerkracht biologie. De uitvoerders hiervan maken daar een filmpje van en/of nemen foto's en publiceren die op een openlijk toegankelijke website waar de klasgenoten naar toe kunnen surfen. De gevolgen zijn natuurlijk groot: het slachtoffer wordt gepest, vernederd… En probeer maar eens zo'n filmpje(s) en/of foto('s) in 1, 2, 3 van het internet weg te halen.

Een beetje in het verlengstuk van het vorige is het belangrijk om even te vermelden dat u best geen enkele, maar dan ook geen enkele, persoonlijke informatie over uzelf deelt met andere Second Life-bewoners. U weet nooit met wie u te doen heeft.

Vooral het risico op verslaving is bij Second Life groot. U wilt uw avatar ontplooien tot een succesvolle persoon en dit door veel Linden-dollars te verdienen en/of door veel vrienden te hebben of door nog andere doelen na te streven die u uzelf voor ogen houdt. U moet er zich bewust van zijn dat dit maar een virtueel leven is dat uw echte leven niet mag schaden. Voor sommigen is hun avatar een verlengstuk van hun eigen persoonlijkheid en brengen ze daardoor veel tijd door in Second Life. U kunt er bijna alles doen en het voornaamste is dat er niemand u iets kwalijk neemt. U kunt er niet dood gaan en de negatieve kanten van het eigen leven zijn weinig of niet voelbaar in Second Life.

Ook in de Second Life-wereld kunt u aan een gokverslaving lijden. Er zijn immers heel wat casino's te vinden.

Enkelen gaan echt wel ver in hun Second Life-ervaring en pompen er maandelijks heel wat geld in. Sommigen zetten zelfs maandelijks 250,00 EUR over in Linden-dollars om zoveel mogelijk hun behoeften te bevredigen. Vaak geven ze dan enkele Linden-dollars weg aan andere avatars om op die manier iets te verkrijgen, bezoeken betalende seksclubs, proberen een eigen luxueuze ruimte te creëren met aangekochte huizen, meubels, … U kunt heel wat zaken gratis krijgen in Second Life, maar wees er ook alert voor dat sommigen daarvan misbruik willen maken. Vaak verkopen avatars zaken die u ook gratis kunt krijgen in Second Life of die al in uw map met bezittingen zitten (Library). Wees dus aandachtig, want sommige bewoners spelen het wel heel slim.

Een echt gevaar kunt u het laatste niet noemen, maar toch vind ik dat u er aandachtig moet mee omspringen. Second Life is in feite een programma dat u moet downloaden en installeren op uw computer. Eenmaal u het geïnstalleerd heeft, kunt u beginnen met spelen. Telkens als u het programma opent en wilt spelen, moet u verbinding maken met het internet en Second Life is een 'zwaar' programma dat heel wat bandbreedte gebruikt. Dus u kunt het al raden, velen spelen Second Life dagelijks een aantal uren en kunnen op een bepaald moment bedrogen uitkomen op het gebied van bandbreedte en dan moeten ze bijbetalen en/of een tijdje internetloos blijven.

10 Eigen Second Life-beleving

Om dit hoofdstuk over Second Life te kunnen opstellen, was het natuurlijk aan te raden dat ik mij niet alleen baseerde op enkele krantenknipsels die dit jaar rond dit onderwerp verschenen. In het begin was ik wat op mijn hoede om Second Life te spelen, omdat ik hier en daar geruchten opving dat het een gevaarlijke en verslavende wereld was. Om me een beter beeld te vormen van deze wereld, kocht ik het recente boek 'Second Life, het officiële handboek'. Ik las de driehonderdtweeënveertig pagina's door en besloot om een Second Life-lid te worden en die zogenaamde tweede wereld eens te gaan verkennen. In het boek staat hier en daar wel iets interessants, maar het is en blijft propaganda voor Second Life. Hoe kan het ook anders, Linden Lab werkte mee aan het tot stand komen van het boek.

Ik installeerde dus Second-Life op mijn computer en begon aan mijn tweede leven. Bij de installatie kon ik mij aansluiten bij een groep van gelijkgezinden en ik koos voor een Nederlandse groep (een Belgische groep bestaat nog niet). Het duurde toch enkele uren voor ik een beetje doorhad hoe alles werkte, ook al had ik het boek gelezen. Het boek is immers aan te raden voor gebruikers die al enkele uren Second Life hebben verkend en is zelfs ook een aanrader voor gevorderde gebruikers die een lang Second Life-leven beschoren zijn. Het boek hielp me echter niet of slechts minimaal met mijn eerste stappen door Second Life. Niet getreurd, want al doende leert men en ook hier was die regel werkelijkheid.

Na mijn registratie op Second Life, kreeg ik dus een standaard avatar die ik kon bewerken. Na twee uurtjes zag mijn avatar er al iets beter uit maar ze voldeed nog niet aan mijn wensen en ik besloot mij te laten inlichten door andere spelers. Dankzij een Nederlandse speelster (of misschien was zij in het echt wel een man) kreeg ik enkele adressen waar ik gratis kon shoppen. Ik ging dit doen en gaf mij avatar nieuwe gratis kleren en een nieuw kapsel. Ik navigeerde wat door Second Life en kwam terecht op een eiland met slechts twee avatars. De avatars zagen er angstwekkend uit maar ze spraken mij onmiddellijk aan en waren erg vriendelijk. Ik vroeg hun enkele dingen over hun Second Life-beleving en het bleek dat ze oude rotten in het vak waren. Ik vroeg hun hoe lang ze al Second Life-lid waren (twee jaar en anderhalf jaar) en hoe ik mijn avatar wat kon aanpassen zodat ze er toch wat normaler ging uitzien. Ik kreeg van één van hen (een Australiër) een compliment: mijn avatar zag er erg goed uit maar ze had enkel een nieuwe 'skin' nodig. Uw 'skin' staat in feite voor het hele lichaam in, inclusief het gezicht (dus hij vond enkel het kapsel en de kleren goed). Ik kreeg van hem (zomaar) vijfhonderd Linden-dollar. Ik bedankte hem en ging shoppen met mijn geld. Ik kocht een nieuwe skin, nieuw haar en nieuwe kleren en zocht wat gratis juwelen die bij het geheel pasten. Ik moet zeggen: ik was en ben trots op het resultaat. Soms koopt u ook bepaalde dingen die niet hetzelfde zijn als op het weergegeven bord (u moet een bord met een weergave van het product aanraken en vervolgens rechts klikken op 'Buy' om iets te kopen). Zo kocht ik eens een paar schoenen en kreeg een vierkante blok rond mijn avatar met reclame voor een bepaalde winkel.

Dit noemen ze nog eens een foute aankoop. Ik kocht een zwart kapsel en kreeg in de plaats een zwarte blok rond mijn hand.

Ik besloot dat ik genoeg had rondgevlogen en koos ervoor om mezelf te teleporteren naar plaatsen die ik willekeurig aanduidde op de Second Life-kaart. Ik vond enkele interessante en leuke plekjes (zoals het eiland van Belgacom, Microsoft, leuke stranden, …) maar ondervond dat er op die plekjes weinig of geen andere avatars te vinden waren. Het viel me op dat vooral de freebies-winkels (waar u dus gratis producten kunt krijgen), de discotheken en de plaatsen rond de seksbars druk bevolkt worden. Jammer voor mensen die mooie dingen creëren in Second Life, maar niet veel bezoek over de vloer krijgen. Langs mijn vliegtocht zag ik heel wat reclameborden en tot mijn verrassing zag ik ook een bord met een opsporingsbericht voor het Britse meisje Madeleine McCann. Ik vind het leuk dat sommigen zich ook hier bewust zijn van de gruwelijke dingen die soms gebeuren in de

echte wereld en vind het goed dat ze via Second Life het opsporingsbericht nog verder proberen te verspreiden in de wereld.

Op de bovenste kubus ziet u een opsporingsbericht met foto's voor het Britse meisje Madeleine McCann.

Second Life dekt zich in met Teen Second Life, een gebied van Second Life dat enkel gereserveerd is voor jongeren. Een gebied waar minder zaken kunnen en mogen dan in de volwassen versie. Als u bij uw registratie uw geboortedatum instelt zodat u bijvoorbeeld een veertienjarige wordt, dan kunt u terecht in Teen Second Life en zogezegd als tiener door uw tweede leven gaan. Een waterdichte beveiliging voor jongeren tegen volwassenen is dit dus zeker niet. Ik vind dat Second Life niets is voor jongeren omdat men in Second Life heel vlug beïnvloed kan worden (bijvoorbeeld door gratis spullen te krijgen) en al heel snel gevraagd wordt naar persoonlijke informatie en om te chatten via MSN. Volgens mij komt ook de vrijheid om alles te doen wat men maar wil de opvoeding van de puber niet ten goede. Waarschijnlijk zijn er tieners die verslaafd raken aan Second Life en er maandelijks (soms zonder hun ouders in te lichten) heel wat geld in pompen. Om te verhinderen dat iemand Second Life speelt op uw computer, kunt u het programma bijvoorbeeld blokkeren via specifieke (gratis) blokkeringssoftware. Een leuk alternatief voor Second Life vind ik het spel 'The Sims'. Het spel is ook erg gevarieerd, modern en het biedt u ook een tweede leven aan. U kunt er ook uw creatieve vaardigheden ontplooien, maar u heeft er natuurlijk niet zoveel mogelijkheden als in Second Life.

Het was leuk en interessant om Second Life te leren kennen. Toch is het een plaats waar u me niet vaak zult terugvinden. Alles wat u doet is tenslotte maar virtueel en daar heb ik niet zoveel voldoening in. Sommigen gaan in Second Life surfen en voelen zich daarbij in het echte leven voldaan; wat ze virtueel doen, beleven en/of voelen ze ook in het echt. Dit kan ik maar moeilijk begrijpen. Wel kan ik begrijpen dat Second Life een verslavend spel is en misschien is die virtuele voldoening daar een gevolg en/of misschien ook een oorzaak van. Of Second Life verder in positieve zin zal evolueren en bijvoorbeeld zal gebruikt worden door het onderwijs, door meer en meer bedrijven, … trek ik in twijfel. Als u het mij vraagt, bezoek ik nog altijd liever de website van Belgacom (overzichterlijker en sneller) dan hun Second Life-eiland.

Voor ik Second Life voorlopig de rug toekeer (want u weet immers nooit hoe de wereld evolueert), wil ik het korte bestaan van mijn avatar zin geven. U kunt op bepaalde plekken

(onder andere ook in de Nederlandse regio) een goed doel sponsoren met Linden-dollars. De resterende honderddertig Linden-dollar die ik nog heb, wil ik dan ook aan een willekeurig goed doel geven. Omdat er op het Nederlandse eiland twee donatiebussen te vinden zijn, donneer ik aan elk vijfenzestig Linden-dollar. Hiermee wil ik Second Life op een nobele manier afsluiten.

Mijn avatar doneert vijfenzestig Linden-dollar in de collectebus van de Flying Doctors en in de collectebus van Stop Aids Now.

Een interessante Nederlandse reportage over Second Life kunt u vinden op http://www.youtube.com waar u een filmpje moet zoeken met de naam 'Droomwereld' dat samengesteld werd door HollandDoc. Dit filmpje interviewt een koppel die beiden elk apart een tweede leven leiden in Second Life. De man heeft een Second Life-vriendin en ontmoet haar in het echt. Ook de virtueel projectontwikkelaarster Ailin Graet (in Second Life: Anshe Chung), die miljonair werd dankzij Second Life, wordt geïnterviewd. Het zevenentwintig minuten en drieëntwintig seconden durende filmpje is het bekijken waard.

In het deel tv-uitzendingen van dit eindwerk vindt u ook informatie terug over een andere en tevens interessante reportage rond Second Life.

DEEL 3 DE BELGISCHE WETGEVING

Er werden nu al een aantal internetgevaren doorlopen maar waarschijnlijk gaat u zich nu afvragen of de Belgische wetgeving enige regelgeving heeft rond informatica en criminaliteit.

Bij bepaalde processen was het duidelijk dat er dringend nood was aan een opname van informaticacriminaliteit in de wet. Daarom verscheen op 3 februari 2001 in het Belgisch Staatsblad de goedgekeurde wet van 28 november 2001 inzake informaticacriminaliteit. Deze wet bevat een reeks bepalingen die de bestaande wetgeving moderniseren zodat er opgetreden kan worden tegen criminaliteit door middel van de computer. In het strafwetboek 'ontstaan' hierdoor vier nieuwe misdrijven:

- valsheid in informatica;
- informaticabedrog;
- datamanipulatie;
- hacking.

In de rechtsleer wordt het begrip informaticacriminaliteit verdeeld in twee 'vormen':

- specifieke informaticacriminaliteit = dit zijn aanvallen tegen computers en netwerken (bijvoorbeeld: verspreiding van computervirussen, computerinbraak, …)
- niet-specifieke informaticacriminaliteit = het informaticasysteem is enkel een middel om een misdrijf te kunnen plegen (bijvoorbeeld: inbreuken op de privacy, verspreiding van kinderpornografie op het internet, …)

De wet inzake informaticamisdrijven beperkt zich echter niet tot de invoering van vier nieuwe misdrijven maar bevat ook enkele strafprocesrechtelijke bepalingen. Dit wil zeggen dat de procureur des Konings de mogelijkheid heeft om gegevens in beslag te nemen, computernetwerken te doorzoeken en experts in te schakelen om mee te werken aan de technische aspecten van deze maatregelen.

Daarnaast is er nog een bepaling die de Belgacomwet (de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven) aanpast. Die bepaling verplicht telecomoperatoren (ertoe) om gedurende een bepaalde periode gegevens bij te houden die (moeten toelaten) gebruikers van hun netwerken (te) identificeren indien zij betrokken raken in een strafonderzoek. Een bewaringsplicht dus.

In principe is het opzettelijk vernielen of beschadigen van computerprogramma's en informaticagegevens door de verspreiding van computervirussen (o.a. via het Internet) strafbaar in België. Dus als uw computer besmet is met een computervirus, dat ook doorgestuurd wordt naar uw vrienden uit uw adresboek, kunt u zelf niet vervolgd worden, omdat u niet de intentie had om de computer van iemand anders te besmetten. Wel moet de maker van het computervirus bestraft worden, maar spijtig genoeg is die meestal moeilijk te achterhalen. De dader/ontwerper van het computervirus kan zich overal ter wereld bevinden. Dus treedt een internationale juridische instantie in werking, zodra een computervirus of een worm verspreid wordt.

In art. 550bis van het Strafwetboek staat ook het misdrijf 'hacking' beschreven. Deze term wordt echter niet letterlijk in de wet gebruikt. In dit artikel wordt er geschreven dat het verboden is om zichzelf toegang te verschaffen tot een informaticasysteem waartoe hij/zij niet gerechtigd is. Wordt dit verbod overtreden, dan maakt de dader kans op een gevangenisstraf van drie maanden tot één jaar en/of een boete van 130,00 EUR tot 125 000,00 EUR.

Hierbij moet echter opgemerkt worden dat de wet bij de beoordeling van de strafbaarheid een onderscheid maakt tussen 'insiders' en 'outsiders':

- De categorie insiders omvat iedereen die weliswaar een bepaalde toegangsbevoegdheid tot een bepaald systeem heeft (bijvoorbeeld werknemers), maar die deze bevoegdheid overschrijdt. Deze categorie is enkel strafbaar indien zij handelen met de bedoeling om te schaden of te bedriegen.
- Voor de categorie outsiders bestaat deze beperking niet, en volstaat een algemeen opzet. Dit is vooral belangrijk omdat hierdoor outsiders, die een systeem kraken 'met goede bedoelingen' (zoals het opsporen van fouten in een systeem), eveneens gestraft kunnen worden. Indien een insider ditzelfde zou doen, zou hij niet gestraft kunnen worden via dit artikel.

Voor beide categorieën is het verboden om gegevens te verzamelen die deze misdrijven mogelijk maken, deze gegevens ter beschikking te stellen of deze te verhandelen. De wetgever wil hiermee vooral de handel in toegangscodes en hacking tools aan banden leggen, door deze eveneens te criminaliseren, indien de hacker de bedoeling heeft om schade aan te richten.

De wet voorziet ook in bestraffing voor pogingen tot hacking, evenals in strengere straffen bij een aantal verzwarende omstandigheden (o.a. dataspionage en tijdsdiefstal).

Ook belangrijk om weten is dat de wet niet vereist dat een veiligheidssysteem doorbroken wordt. De ongeoorloofde toegang is dus ook strafbaar indien het computersysteem slecht of zelfs helemaal niet beveiligd is.

Niet alle landen hebben een wet rond informaticacriminaliteit. Zo kregen de Taiwanese maker van het Tsjernobyl-computervirus en de Filippijnse bedenker van de lovebug geen of een minieme straf omdat hun wet nog niet werd aangepast aan de hedendaagse informaticamaatschappij. Toch zijn al heel wat landen op de goede weg (waaronder ook België) en werden reeds enkele hackers en computervirusmakers gevat. Een overzichtje van enkele computervirusmakers en hackers die zowel in binnen- als buitenland tegen de lamp liepen:

- Een bekend geval in België is dat van Frans Devaere uit Lovendegem, alias RedAttack. In 2000 wordt hij doorverwezen naar de correctionele rechtbank van Gent voor inbreuken op de Belgacomwet. Hij riskeert een veroordeling van 247,89 EUR tot 247 893,52 EUR voor het hacken van verschillende computerbestanden van Belgacom Skynet in augustus '99. Hem wordt aangewreven dat hij met opzet kennis heeft genomen van gegevens inzake telecommunicatie die betrekking hebben op andere personen. Kort na zijn inbraak bij Belgacom doet RedAttack hetzelfde in het zogenaamd beveiligde systeem van de Generale Bank. Ook hier stelt hij de gaten in grote computersystemen aan de kaak. Hij wijst (met goede bedoelingen) in oktober 2000 op de gevaren van pc-bankieren: zonder moeite kon hij de paswoorden achterhalen van BBL-klanten. RedAttack biedt zowel de regering als bedrijven zijn diensten aan om hacking te voorkomen. Toch was de toenmalige premier Dehaene niet tevreden toen zijn computersystemen gehackt werden door RedAttack. Naar eigen zeggen ontmaskert RedAttack in 1999 een aantal pedofiele leraren uit Brugge. In december 2000 veroordeelt de Gentse strafrechter hem tot een boete van 991,57 EUR en 0,02 EUR (toen één frank) morele schadevergoeding aan Skynet. Eind mei 2001 wordt RedAttack opgepakt omdat hij opnieuw binnendrong in de websites van verschillende bedrijven (waaronder ook de website van het Kuifje-imperium). Daarbij waren zijn bedoelingen lang niet zo

nobel als bij zijn eerste stunts en wiste hij gegevens op de websites. Na een maand komt Devaere, die van een complot van een ex-zakenpartner spreekt, op borg vrij. In november 2002 én in februari 2003 moet hij zich telkens weer verantwoorden voor nieuwe gevallen van hacking. Verbitterd zegt hij de computerwereld vaarwel omdat hij het zat is dat anderen onder de naam RedAttack inbreuken plegen of naar hem verwijzen. Nochtans worden in juni 2003 sporen van hacking aangetroffen op zijn computers. Al houdt hij zijn onschuld staande, in december 2003 wordt hij veroordeeld tot één jaar voorwaardelijke celstraf en een boete van 14 873,00 EUR.

- In België krijgt David N. (vijfentwintig jaar) uit Duffel eind mei 2001 een boete van 2 478,94 EUR van de correctionele rechtbank in Mechelen. Deze boete kreeg hij voor het doorsturen van een computervirus naar een ex-liefje dat hij via een datingsite had leren kennen. Het meisje kon haar computer maandenlang niet gebruiken en dat veroorzaakte problemen bij haar studies aan de kunstacademie.

- De eerste Nederlander, die veroordeeld werd voor een computermisdrijf, was de maker van computervirus Koernikova. De twintigjarige student kreeg in 2001 in hoger beroep een werkstraf van honderdvijftig uur.

- Jay Satiro, een negentienjarige Amerikaanse computerhacker, werd eind 1999 veroordeeld tot een jaar gevangenisstraf en vijf jaar zonder pc. Satiro kraakte het computernetwerk van America Online. Deze softwaregigant wilde niet kwijt op welke wijze zijn computers werden gehackt of wat het effect daarvan was, wel wilde hij kwijt dat het hem 50 000 USD (36 231,88 EUR) kostte om de schade te herstellen.

- In 2002 werd in de Verenigde Staten de drieëndertigjarige David Smith, maker van het computervirus Melissa (maart 1999), veroordeeld tot een boete van 5 000 USD (3 623,19 EUR) en een gevangenisstraf van twintig maanden. Hij gaf toe dat hij een enorme fout had gemaakt. Smith had ook een gevangenisstraf van vijf jaar kunnen krijgen maar kreeg strafvermindering omdat hij de autoriteiten hielp met het bestrijden van andere computervirussen.

- Microsoft, die regelmatig aangevallen wordt door hackers, is het beu. Bill Gates loofde begin mei 2004 een beloning uit van een kwart miljoen dollar (181 159,42 EUR) voor de tip die tot de aanhouding zou leiden van de maker van het Sasser-computervirus. De 'vrienden' van de achttienjarige Sven J. uit Nedersaksen konden aan dit geld niet weerstaan en gaven hun vriend aan. Sven J. riskeert een celstraf van vijf jaar.

Daarnaast mag iemand zonder uw toestemming geen persoonlijke informatie op het internet over u verspreiden en/of er gebruik van maken. Hierbij is het mogelijk om u te beroepen op de Europese richtlijn 95/46/EG 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 (Belgisch Staatsblad - 03 februari 1999). Hieruit kan worden afgeleid dat het normaal gezien verboden is om u ongevraagde publiciteit te versturen per e-mail (buiten enkele uitzonderingen). De adverteerder moet dus in feite eerst uw toestemming vragen alvorens hij reclame via e-mail kan sturen en/of uw persoonlijke gegevens doorgeeft aan derden. Bij dergelijke e-mails is de verstuurder onder andere verplicht u in te lichten over zijn identiteit. Daarnaast heeft u ook altijd het recht om uw eventuele eerder gegeven toestemming te annuleren.

Vaak wordt de vraag gesteld of virtuele kinderporno, zoals in Second Life, strafbaar is volgens de Belgische wetgeving. Er bestaat geen specifieke regelgeving rond virtuele kinderpornografie in Second Life, maar wel een algemene regelgeving rond kinderporno. Die regelgeving duidt aan dat het bekijken van kinderporno op zich niet strafbaar is, maar het bewust verspreiden en bewaren van kinderporno wel. Er wordt ook bij vermeld dat het hier niet hoeft te gaan om echte kinderen. De bezitter van afbeeldingen van seksuele handelingen, waarin een minderjarige wordt voorgesteld, is strafbaar. Deze minderjarige hoeft

geen reële persoon te zijn, het kan bijvoorbeeld ook een avatar zijn. Gelukkig zijn er in België nog geen klachten geweest omtrent virtuele kinderporno.

Ook is het belangrijk dat u weet dat er in België het 'Federal Computer Crime Unit' (FCCU) bestaat bij de Federale Gerechtelijke politie (ook internetpolitie genaamd). Deze cel trekt dagelijks ten strijde tegen informaticacriminaliteit. Het FCCU en de Federale Overheidsdienst Economie, KMO, Middenstand en Energie hebben samen een meldpunt opgericht voor misdrijven op of via het internet. Het internetadres van dit meldpunt is http://www.ecops.be. Welke informaticacriminaliteit u ook meldt (een site van kinderporno, inbraak door een hacker, …), het eCops-team zorgt ervoor dat uw melding door de bevoegde dienst wordt onderzocht.

DEEL 4 BEWUSTMAKING VAN DE INTERNETGEVAREN

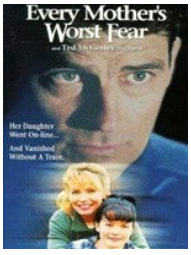
In het theoretische gedeelte van dit eindwerk vindt u de uitleg over wat de grootste internetgevaren voor jongeren zijn. Bij elk hoofdstuk werden ook tips gegeven om zich te beschermen tegen die gevaren. Het is belangrijk dat iedereen, die toegang heeft tot het internet, zich bewust is van deze internetgevaren. De voorbije jaren zijn hiervoor reeds een aantal initiatieven genomen. Hieronder vindt u een greep uit de interessantste campagnes, tv-uitzendingen, films en artikels omtrent de internetgevaren. Daarnaast vindt u ook meer uitleg over de multimedia dvd die ik heb samengesteld om de jongeren bewust te maken voor welke internetgevaren zij het meest vatbaar zijn.

1 Films

Het grote voordeel van films is dat ze mensen (en vooral jongeren) erg aanspreken. Ze worden lang in het geheugen gehouden en geven de zaken visueel weer. Een film kan tevens een goede inleiding zijn voor een studieobject (bijvoorbeeld voor de cd-rom rond internetgevaren [zie verder]). Indien dit het geval is, is een nabespreking wenselijk, waardoor een goed leergesprek kan plaatsvinden dat de leerlingen heel wat doet inzien.

Alle films handelen over internetgevaren. Ik heb alle films bekeken en kwam tot het besluit dat niet alle films geschikt waren voor jongeren. In dit hoofdstuk heb ik elke film kort toegelicht.

1.1 Every mother's worst fear



'Every mother's worst fear' is een film die in 1998 werd geregisseerd door Bill L. Norton. De film is een (±) 91 minuten durend drama met als hoofdrolspelers Cheryl Ladd, Jordan Ladd en Robert Wisden.

Martha, een zestienjarig meisje woont samen met haar hardwerkende moeder, heeft gescheiden ouders en verblijft in de weekends bij haar vader. Ze heeft het enorm moeilijk met de scheiding en daarbovenop laat haar vriendje haar in de steek. Haar moeder maakt heel veel overuren en is dus weinig thuis. Martha zoekt troost en vriendschap in chatrooms. Op de chatroom doet ze haar verhaal over haar thuissituatie en vertelt ze hoe moeilijk ze het ermee heeft. Het hoofd van een pedofielennetwerk 'luistert' aandachtig mee naar wat Martha allemaal te vertelen heeft en hij schrijft ook al haar gegevens op. Hij zorgt ervoor dat één van z'n pionnen contact heeft met haar en dat dit contact tot een afspraak in het echte leven leidt. Martha krijgt een vliegtuigticket opgestuurd en loopt op een gegeven moment weg van huis om af te spreken met haar 'chatvriend' Drew. Het afspraakje loopt echter niet zoals ze verwachtte en ze wordt door Drew ontvoerd. Wanneer haar 'chatvriend' Drew haar niet meer aankan, komt ze terecht bij het hoofd van het pedofielennetwerk. Martha raakt verstrikt in een pedofielennetwerk en men kan op het internet bieden om haar te kopen. Haar ouders doen er alles aan om Martha terug te vinden en ook de FBI wordt ingezet.

Dit is een goede film die duidelijk maakt dat u ontzettend voorzichtig moet zijn met de persoonlijke informatie die u geeft op het internet. Er is duidelijk te zien dat niet iedereen op een chatbox goede bedoelingen heeft en dat mensen zich er soms anders voordoen. De film geeft goed weer hoe het netwerk in elkaar zit en hoe moeilijk het is om bij de echte dader terecht te komen: zijn telefoonnummer en IP-adres zijn niet te achterhalen, harde schijven met eventuele sporen worden gewist, sporen leiden naar verschillende pionnen, …

Hoewel de film uit 1998 dateert, vind ik dat hij (relatief) nog goed mee kan met deze tijd (qua computergebruik, internet, …). Uit alle films, die in dit deel worden besproken, vind ik deze persoonlijk de beste. Er staat vermeld dat de film geschikt is vanaf 16 jaar, maar ik vind dat hij al geschikt is voor jongeren vanaf de eerste graad. Een aanrader…

Ik heb ontzettend veel zoekwerk moeten doen om deze film te kunnen bemachtigen. Uiteindelijk heb ik hem via een website tijdens een Nederlandse uitverkoop kunnen kopen. Heeft u deze film eens nodig, dan kunt u gerust bij mij terecht (valerie_pauwelyn@msn.com). In principe is de film enkel op VHS beschikbaar, maar ik heb hem ondertussen op een dvd gekopieerd (om kwaliteitsverlies te vermijden en voor persoonlijk gebruik).

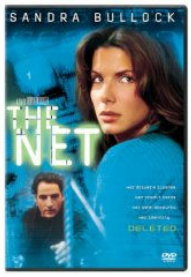
1.2 Net.Games

'Net.Games' is een film die in 2003 geregisseerd werd door Andrew van Slee. De film is een ongeveer 101 minuten durende thriller met als hoofdrolspelers: C. Thomas Howeel, Ed Begley Jr. en Marina Sirtis.

Adam is een succesvolle zakenman met veel goede vrienden en een goed huwelijk. Zijn vrouw (Jennifer) werd echter een tijdje geleden verkracht en is nog niet klaar om de liefde met Adam te bedrijven. Een vriend van hem biedt een oplossing: cyberseks: geen lichamelijk contact, alleen fantasie. Op de chatbox maakt Adam kennis met een psychopate die de schuilnaam 'Angel' heeft. Angel heeft via internet op een of andere manier toegang tot alle gegevens van Adam. Na een paar keer cyberseks, wil ze Adam in het echt ontmoeten. Ze doet dit namelijk met meerdere mannen, waarbij ze hen na de seks vermoordt. Adam wil ermee ophouden maar Angel chanteert hem op alle mogelijke manieren. Adam raakt verstrikt in een smerig spel en moet vechten voor zijn leven en voor alles wat hem lief is.

Deze film geeft mooi weer hoe u kunt getraceerd worden via uw IP-adres. Angel komt alles te weten over Adam en kan hem chanteren thuis, op het werk, … De film heeft als boodschap dat u waakzaam moet zijn op het internet. Deze film is geschikt voor zestien plus. De boodschap van de film zit wel goed, maar ik vind hem niet echt toonbaar in een schoolomgeving omdat er ontzettend veel seks in voorkomt.

1.3 The Net



De (±)109 minuten durende thriller 'The Net' werd in 1995 geregisseerd door Irwin Winkler. De hoofdrolspelers van deze film zijn Sandra Bullock, Jeremy Northam en Dennis Miller

Angela Bennett (Sandra Bullock) is een jong computergenie dat een geïsoleerd leven leidt; ze heeft weinig sociale contacten. Ze zoekt computervirussen in programma's en probeert die te verwijderen zodat bepaalde producten/spelletjes virusvrij op de markt kunnen komen. Op een dag krijgt ze een programma doorgestuurd dat er in eerste instantie onschuldig uitziet, maar dat u, mits de juiste behandeling, toegang geeft tot geheime informatie van ziekenhuizen, bedrijven, banken, … Dale, een collega van Angela en de man die haar het bewuste programma doorstuurde, wordt vermoord (in eerste instantie lijkt het op een gewoon ongeval) en tijdens haar vakantie in Mexico ontsnapt Angela zelf aan een aanslag. Wanneer Angela thuiskomt, blijkt haar identiteit gestolen en ook alles waarmee ze zich kon verifiëren is weg: haar identiteitskaart, bankkaart, huis, auto, … Daarbovenop komt nog eens dat ze een andere identiteit gekregen heeft, die van een misdadigster. Angela begint haar speurtocht naar de dader, maar dit verloopt niet vlekkeloos want niemand gelooft haar verhaal

'The Net' geeft weer hoe afhankelijk we geworden zijn van computers en hoe al onze informatie er tegenwoordig op terug te vinden is. Dat iemand toegang heeft tot al deze informatie en deze eventueel kan beïnvloeden leidt natuurlijk tot een enorme machtspositie. In de film wordt die machtspositie gebruikt om de virusscanner Gatekeeper te promoten, maar in dit programma zit een lek dat ervoor zorgt dat de dader tot alle 'beveiligde' computers toegang krijgt. De film geeft heel goed weer hoe gegevens gemanipuleerd kunnen worden via het internet en welke verstrekkende gevolgen dit soms heeft. Een mooie, boeiende en spannende film die naar mijn mening geschikt is voor jongeren vanaf de eerste graad. Het minpuntje van deze film is dat hij niet echt gericht is op de internetgevaren voor jongeren.

1.4 Hard Candy

'Hard Candy' is een film uit 2005 die in de categorieën drama en thriller valt. De (±) 103 minuten durende film werd geregisseerd door David Slade. Volgende hoofdrolspelers zien we aan het werk: Patrick Wilson, Ellen Page en Sandra Oh.

Hard candy is de internetterm voor een minderjarig meisje en tevens de naam van een film die zich vooral tussen de vier muren van een appartement afspeelt. De veertienjarige Hayle spreekt af met een modefotograaf (Jeff) die ze via een chatbox heeft leren kennen en ze gaat mee naar zijn appartement. Als kijker denkt u dat het fout zal aflopen met Hayley, maar uiteindelijk draaien de rollen om en is het Jeff die vastgebonden en geterroriseerd wordt. Hayley verdenkt Jeff van pedofiele praktijken en moord op haar vriendin en drijft hem tot het uiterste om hiervan bewijzen in handen te krijgen. Jeff is een pedofiel, maar of hij effectief de dader is van de moord op haar vriendin, blijft een open vraag…

De flaptekst van de dvd schept de verwachting dat deze film gaat over een meisje dat een man leert kennen via een chatbox en vervolgens met hem afspreekt en meegelokt wordt naar zijn appartement. Toen ik de film bekeek, had ik ook die verwachting in mijn hoofd, maar het draaide helemaal anders uit. Ik vind dit één van de slechtere films die meer thuis hoort bij het genre psychologische thriller. Deze film is ook minder geschikt voor leerlingen omwille van het seksuele geweld.

1.5 Cyberseduction, His Secret Life

'Cyberseduction, His Secret Life' is een film die in 2005 geregisseerd werd door Tom McLoughlin. De film is een (±) 87minuten durend drama met als hoofdrolspelers Jeremy Sumpter, Kelly Lynch en Lyndsy Fonseca.

Deze film gaat over een jongen, Justin, die we kunnen omschrijven als een gewone leerling. Justin blinkt uit in zijn zwemprestaties en hij is één van de gelukkigen die mag aansluiten bij het staatsteam. Hij bevindt zich in een normale gezinssituatie en heeft een broer en een vriendin. Op school stijgt Justin's populariteit en hij ontmoet er Monica. Die avond bekijkt hij Monica's website, waar heel wat uitdagende en sexy foto's en filmpjes terug te vinden zijn. Justin geeft zijn ogen de kost en later krijgt hij van een vriend ook enkele websites doorgestuurd, waar hij uitdagende foto's vindt van andere meisjes. Justin raakt geobsedeerd door deze foto's en brengt heel wat uren door achter zijn computer. Zijn school- en zwemprestaties lijden eronder want hij komt amper tot slapen toe. Ook zijn broer raakt hieraan verslaafd met alle gevolgen vandien.

In de film wordt duidelijk weergegeven hoe Justins online-pornografie zijn leven en tevens zijn relaties beïnvloedt. Justins ouders proberen z'n probleem op te lossen door zijn computer te verhuizen van z'n kamer naar de woonkamer. Toch slaagt Justin erin om z'n ou-

ders nog te misleiden door in de bibliotheek en het internetcafé zijn bezigheden verder te zetten. 'Cyberseduction, His Secret Life' is een film die goed weergeeft wat het probleem is en wat de gevolgen ervan zijn. Persoonlijk vind ik deze film geschikt voor leerlingen vanaf de 2de graad.

Deze film sluit niet perfect aan bij de onderwerpen die in het theoretische deel van dit eindwerk werden verduidelijkt, omdat hij hoofdzakelijk gaat over online pornografie. Toch kan deze film gebruikt worden als voorbeeld van internetverslaving en haar gevolgen. U kunt de leerlingen dan duidelijk maken dat Justin verslaafd is aan online pornografie maar dat u ook internetverslaafd kunt worden door te chatten, Second Life, online pornografie, online spelletjes, ….

Nergens heb ik een vermelding gevonden dat deze film op VHS of dvd beschikbaar is. Ik heb deze film opgenomen toen hij vertoond werd op televisie. Als iemand deze film nodig heeft, kan hij/zij gerust bij mij terecht. Ik heb hem op een dvd gebrand.

2 Tv-uitzendingen

Tv-uitzendingen spelen kort op de bal en informeren de mensen over actuele thema's. Beelden zeggen vaak meer dan woorden…

Hieronder vindt u een samenvatting van enkele recente tv-uitzendingen over internetgevaren voor jongeren. De tv-uitzendingen werden op een dvd geplaatst en zitten in de eindwerkdoos. Veel kijkplezier.

2.1 Algemeen: de gevaren van het internet

Minister Vanvelthoven over het Suske en Wiske album 'De Sinistere Site'

Programma: Knevel & Van den Brink
Zender: Nederland 1
Uitzenddatum: 14 mei 2007
Duur: 15 minuten en 48 seconden
Titel van de uitzending op dvd:
'Knevel & Van den Brink 14/05/2007'

Knevel & Van Den Brink is een Nederlands praatprogramma waar – meestal met bekende personen - gedebatteerd wordt over de actualiteit. In de uitzending van maandag 14 mei 2007 was de Belgische minister van Werk en Informatie Peter Vanvelthoven aan het woord.

Minister Vanvelthoven kwam op het idee om kinderen te waarschuwen voor internetgevaren aan de hand van een Suske en Wiske album. Het stripalbum 'De Sinistere Site' is vooral bedoeld voor leerlingen uit de laatste graad van de basisschool. Het stripalbum probeert op een leuke manier de kinderen tips te geven om zich te wapenen tegen internetgevaren. In België werden al tweehonderd albums verspreid via de basisscholen en dit met de bedoeling dat er in de klas rond gewerkt zou worden.

Minister Vanvelthoven kwam in het Nederlandse praatprogramma terecht omdat het Suske en Wiske album 'De Sinistere Site' ook in de Nederlandse basisscholen verspreid zal worden.

Veiliger internetten met Suske en Wiske

De striphelden Suske en Wiske gaan nu ook Nederlandse kinderen op de basisschool veilig leren internetten. De stichting *Kennisnet ICT op School* verspreidt de speciale uitgave *Suske en Wiske en de sinistere site*. De strip is vorig jaar gemaakt door Studio Vandersteen op verzoek van de Belgische staatssecretaris voor Informatisering Peter Vanvelthoven. Het stripverhaal draait rond een tovenaar die kinderen via een betoverde website naar zich toe lokt, zo valt te lezen op de website van de stripserie. Wiske trapt in de val en wordt het internet in "geflitst". De andere striphelden doen er alles aan om haar te redden. Aan de hand van hun avonturen wordt verteld over de gevaren van internet en hoe kinderen die kunnen vermijden.
Info: suskeenwiske.ophetwww.net

Bron: Jobat (19 mei 2007)

2.2 Jongeren en chatten

De digitale generatie: internet als vriend en vijand

Programma: Netwerk
Zender: Nederland 1
Uitzenddatum: 30 oktober 2005
Duur: 29 minuten en 13 seconden
Titel van de uitzending op dvd:
'Netwerk - De digitale generatie 30/10/2005'

Een reportage over de digitale generatie waarin duidelijk gemaakt wordt wat jongeren zoal 'uitspoken' op het internet. Deze reportage kwam er naar aanleiding van de arrestatie van een man uit het Nederlandse Beverwijk die ervan verdacht wordt vijfentwintig meisjes te hebben gedwongen tot webcamseks. De meisjes moesten zich uitkleden en masturberen voor de webcam. De man dwong de meisjes steeds verder en verder te gaan door middel van chantage. Hij had namelijk alle voorgaande beelden opgenomen en dreigde die op het internet plaatsen.

In de reportage vertellen enkele kinderen en jongeren over hun internetbelevenissen: hoe ze met elkaar communiceren via het internet en met welke narigheden ze er soms geconfronteerd worden. Zo heeft bijvoorbeeld de tiener Marie Louise, een jong model, net zoals vele anderen (> 1 miljoen mensen) een profielpagina bij Sugababes. Sugababes is een Nederlandse profielsite waar jonge meisjes een persoonlijke webpagina kunnen maken waar ze zichzelf beschrijven, foto's van zichzelf op die pagina plaatsen, ... Via die site kwam Marie Louise reeds in contact met mannen die zich uitgaven als fotograaf. Ze vroegen haar om voor de webcam te strippen zodat ze konden zien of ze in aanmerking kwam voor een van hun zogezegde fotoreportages. Gelukkig was Marie Louise niet zo naïef en blokkeerde ze die mannen. Ze gaf hun schuilnamen door aan de moderators van Sugababes die ervoor zorgden dat deze mannen geen toegang meer hadden tot de profielpagina's en op een zwarte lijst terechtkwamen. Ook de heer Hendriks van Sugababes komt aan het woord en vertelt dat er enkele moderators toekijken op de profielsite. De moderators grijpen in wanneer het op Sugababes uit de hand loopt en als de taal of de foto's te extreem worden. De heer Hendriks verduidelijkt waar bij hen de grens ligt tussen wat kan en wat niet kan.

Bamber Delver, directeur van stichting De Kinderconsument, levert ook een bijdrage in de reportage. De heer Delver organiseert in Nederland voorlichtingsbijeenkomsten voor zowel ouders als kinderen. In de reportage maakt hij duidelijk dat er een enorme generatiekloof is tussen deze twee generaties. Ouders hebben vaak geen basiskennis over de nieuwe media en deze is toch essentieel om er met hun kinderen te kunnen over praten. Ouders moeten gaan inzien dat het internet belangrijk is voor kinderen: voor hun huiswerk, voor hun sociale contacten, … en dat ze het internet dus niet zomaar van de tafel kunnen vegen. Ook moeten de ouders in de gaten houden wat hun kinderen op het internet doen en dit gebeurt volgens de heer Delver veel te weinig. Ook maakt de heer Delver duidelijk dat niet iedereen op het internet goede bedoelingen heeft.

Ook de heer van Kokswijk, een Nederlandse communicatiewetenschapper, komt in de reportage aan het woord. In het kader van een Europees onderzoek heeft hij met honderden jongeren gechat en hun wereld geanalyseerd. De heer van Kokswijk had het vooral moeilijk met de turbotaal die jongeren tijdens het chatten gebruiken: de ballast van de Nederlandse taal wordt weggegooid, het woordgebruik is een mix van Nederlandse en Engelse woorden en de tekst wordt vaak geschreven zoals hij uitgesproken wordt. Jongeren, die uren chatten, zijn volgens de heer van Kokswijk vaak jongeren die geen aansluiting meer hebben met hun ouders en die met iemand over hun problemen willen praten.

Mevrouw de Graaf van de Rutgers Nisso Groep (kenniscentrum seksualiteit) doet onderzoek naar seks bij jongeren onder de vijfentwintig jaar. Zij ontdekte dat jongeren vaak over seks iets opzoeken op het internet, dat ze cyberseks hebben en zelfs afspraakjes regelen via het internet.

Ook zedenrechercheur van Brunschot komt aan het woord in de reportage. Hij vertelt dat de berichtengeschiedenis, de schermafdrukken en het tijdstip van de aanwezigheid op het internet (van de dader) belangrijk zijn wanneer u een internetmisdrijf wilt aangeven.

Dit is een zeer goede reportage voor mensen die graag wat meer willen te weten komen over de digitale generatie. De reportage heeft wel betrekking op Nederlandse jongeren maar u kunt de lijn doortrekken naar Vlaamse jongeren. Ook in Vlaanderen hebben we MSN, chatboxen en profielsites (bijvoorbeeld Redbox). De reportage is zeker en vast een aanrader, zeker voor ouders en leerkrachten die nog weinig weten over de internetactiviteiten van de jeugd.

Resultaten van een enquête over het chatten van Vlaamse jongeren

Programma: Koppen
Zender: Één
Uitzenddatum: 27 maart 2007
Duur: 37 minuten en 18 seconden
Titel van de uitzending op dvd:
'Koppen – Enquête over chatten 27/03/2007'

De Vlaamse tiener zit gemiddeld 86 minuten per dag op het internet. Koppen hield in samenwerking met Het Nieuwsblad en Child Focus een enquête bij Vlaamse jongeren over hun chatgedrag. Op die manier krijgen we een beeld over het aantal uren dat jongeren chatten, of er een verschil is tussen het chatgedrag van jongeren naargelang hun ouders gescheiden zijn of niet, of de jongeren afspreken met nooit eerder geziene chatvrienden, …

In de speciale Koppen-uitzending worden de resultaten van de enquête bekend gemaakt. In de Koppen-studio zelf praten kinderpsychiater Peter Adriaenssens en Dirk Depover van Child Focus over deze resultaten, met als gespreksleider Annelies Van Herck. Ook Wim De Vilder doet een bijdrage in deze uitzending en interviewt een aantal jonge frequente chatters over hun belevenissen. Ook het verhaal van Kim komt naar voren. Kim is een meisje dat op zestienjarige leeftijd in het echt afsprak met iemand die ze op een chatbox had leren kennen. Tijdens het afspraakje werd ze meegelokt naar zijn kot, waar ze verkracht werd. In de reportage komen ook twee moderators van een chatbox aan het woord.

Een interessante uitzending die u een idee en cijfers geeft over het chatgedrag van Vlaamse jongeren.

2.3 Cyberpedofilie

Het computerseks-proces gaat van start

HET NIEUWS

Programma: Het Nieuws
Zender: VTM
Uitzenddatum: 6 september 2006
Duur: 2 minuten en 38 seconden
Titel van de uitzending op dvd:
'Het Nieuws – Cyberpedofiel 06/09/2006'

Dit nieuwsbericht gaat over het computerseks-proces dat op 6 september 2006 van start ging. Het proces ging over een tweeëntwintigjarige man die zich tegenover de rechter moest verantwoorden voor zedenfeiten via het internet. De man deed zich op chatboxen voor als een tienjarige jongen en dwong een veertigtal minderjarige meisjes zich uit te kleden voor de webcam; sommigen moesten zichzelf ook aanraken. Gelukkig is er nooit fysisch contact geweest tussen de man en een van de meisjes.

De dader wordt beticht van aanranding van de eerbaarheid met geweld omdat hij de meisjes moreel zou hebben verplicht om zich uit te kleden. De man riskeert tot 15 jaar cel.

Uitspraak in het computerseks-proces

Programma: Het Journaal
Zender: Één
Uitzenddatum: 4 oktober 2006
Duur: 44 seconden
Titel van de uitzending op dvd:
'Journaal – Cyberpedofiel 04/10/2006'

De tweeëntwintigjarige man, die terecht stond in het computerseks-proces (zie uitzending van Het Nieuws van 6 september 2006), werd veroordeeld tot een werkstraf van 240 uur en een verbod om het internet voor privédoeleinden te gebruiken.

Undercover in de wereld van de cyberpedofielen

Programma: Panorama
Zender: Canvas
Uitzenddatum: 4 maart 2007
Duur: 41 minuten en 37 seconden
Titel van de uitzending op dvd:
'Panorama – De wereld van de cyberpedofielen 04/03/2007'

Panorama brengt een reportage van eigen makelij. Ze dringen met verborgen camera's door in de wereld van de cyberpedofielen. We zien in de aflevering enkele getuigenissen van Vlaamse jongeren, die reeds het slachtoffer werden van cyberpedofilie. Telkens krijgen we ook te horen welke straf de betreffende cyberpedofiel kreeg voor zijn daden.

We krijgen het verhaal van Marie te zien. Ze was elf jaar toen een onbekende man met haar begon te chatten. In eerste instantie dacht Marie dat hij een schoolkameraadje was, maar toen de man een blote foto van zichzelf stuurde, bleek dit niet zo. Marie was geschrokken, telefoneerde naar haar vader en vertelde wat ze had meegemaakt. Maries vader kwam onmiddellijk naar huis en verwittigde de politie. De vader begon in naam van Marie te chatten en de man stuurde tijdens het chatgesprek een filmpje door, waarin hij masturbeerde en hij vertelde dat hij graag seks zou hebben. Na afloop van het filmpje toonde de man zijn gezicht via de webcam. Die avond nog werd de man opgepakt. Hij had een blanco strafblad en kreeg hierdoor een lichte straf: 12 maanden voorwaardelijk en verplichte psychiatrische behandeling. Ook werd hem alle contact met Marie en haar vader verboden.

Ook Elize doet haar verhaal. Toen ze vijftien was, kreeg ze via de website van haar persoonlijke webpagina een e-mail van een achtendertigjarige man. Door haar voortdurend complimentjes te geven, wist de man het vertrouwen van Elize te winnen. Even later begon hij met expliciete seksuele taal. In het begin zei Elize dat ze dat niet fijn vond, maar ze reageerde na een tijdje toch op zijn uitspraken en antwoordde op zijn vragen. Zoals Elize zelf

zegt, werd ze als het ware in zijn gesprekken meegesleurd. De man vroeg een topless foto en Elize voelde zich hiertoe verplicht. Via de webcam stuurde ze haar naaktfoto door. De man vroeg ook om met Elize eens af te spreken; zover kwam het niet… De verantwoordelijke van de website verwittigde Elizes vader. Hij vertelde hem dat Elize naaktfoto's had verstuurd naar een oudere man, die ook andere meisjes precies op dezelfde manier had benaderd. De vader legde meteen klacht neer bij de politie. De man kwam er met een lichte straf vanaf: hij mocht drie jaar niet meer surfen op het internet en moest zich laten begeleiden door een psychiater. Elize vindt dat de man wel een zwaardere straf verdient voor wat hij allemaal heeft aangericht.

Een ander verhaal is dat van Julie die met een negenenvijftigjarige man chatte. Toen die man na enkele chatgesprekken haar vertrouwen had gewonnen, gaf hij al gauw seksuele opmerkingen en begon hij haar seksuele vragen te stellen. Julie werd naar eigen zeggen niet verliefd op die man, maar ze aanzag hem meer als een vertrouwenspersoon. De man stelde voor dat ze elkaar zouden ontmoeten en Julie gaat effectief op dit aanbod in. Julie en de man gaan een eindje wandelen op een afgelegen plek en al snel valt de man haar lastig en verkracht haar. Julie durft haar ouders niets te vertellen over de verkrachting. Haar moeder leest toevallig een berichtje, waarin Julie een vriendin vertelde over de verkrachting. Julies ouders legden onmiddellijk klacht neer bij de politie. Julie moest twee jaar opgenomen worden in een psychiatrische instelling, waar ze een paar keer zelfmoord probeerde te plegen. De negenenvijftigjarige man werd over de hele lijn schuldig bevonden. Toch moest hij niet naar de gevangenis. Hij kreeg twee jaar voorwaardelijk en moest zich laten begeleiden door een psychiater. Julie kreeg vijfduizend euro morele schadevergoeding.

Volgens velen zijn deze relatief lage straffen te licht voor cyberpedofielen. Deskundigen leggen de reden bij de wet, die nog onvoldoende het fenomeen cyberpedofilie opgenomen heeft. Vaak krijgen cyberpedofielen een voorwaardelijke gevangenisstraf, keren ze terug naar huis en worden ze enkel op bevel van de rechter een tijdje door een maatschappelijk werker gevolgd.

Lieve Dams, gerechtspsychiater, bezorgt de reportage een meerwaarde door haar inbreng. Ze vertelt onder andere dat de slachtoffers van cyberpedofilie in tweestrijd met zichzelf leven. De slachtoffers zien enerzijds dat de dader hun vertrouwen geschonden heeft, dat hij hen pijn deed en dat hij iets illegaal deed, maar aan de andere kant is er ook een enorme loyauteit. De man, die hen tenslotte beschadigd heeft, is ook lief en aardig geweest op het moment dat zij dat nodig hadden. Dit inwendige conflict is iets waar therapeuten de slachtoffers mee moeten helpen. Uit de meeste chatgesprekken blijkt dat de meisjes wel wisten dat de man een pak ouder was dan zij, maar dat ergerde hen niet omdat ze op zoek waren naar een soort vaderfiguur die hun positieve aandacht kon geven. Vroeger gingen pedofielen onder andere in speeltuinen en in het zwembad op zoek naar hun slachtoffers, tegenwoordig gebeurt dit via het internet. Pedofielen hebben immers het gevoel dat ze via het internet niet te lokaliseren zijn. Via het internet gaat het ook een stuk makkelijker om contact te leggen met minderjarigen. Seksueel 'getinte' chatgesprekken zijn voor cyberpedofielen vaak een tussenstap voor het echte fysiek contact waar ze op aansturen.

Peter De Waele van de Brusselse Gerechtelijke Politie komt in de reportage aan het woord. De heer De Waele werkt al tien jaar voor de cel pedofilie en verhoort zowel slachtoffers als daders. Hij ondervindt dat het ultieme droombeeld van cyberpedofielen het effectief misbruik is. Cyberpedofielen nemen de beelden, die ze via het internet van meisjes hebben, op om twee redenen: omwille van het feit dat ze er zichzelf mee kunnen bevredigen en omwille van het chantage-aspect. Meisjes zijn immers bang dat de foto's en/of filmpjes op het internet zouden verspreid worden en dat hun ouders ervan op de hoogte zouden worden gebracht. Volgens Peter De Waele wisselen pedofielen dergelijke foto's en/of filmpjes met elkaar uit en dit doen ze vooral via chatboxen. In de uitzending zien we ook de opbrengst van de huiszoeking van een kinderpedofiel (duizende video's met kinderporno).

Luc Beirens van de Federal Computer Crime Unit vertelt in een interview dat de politie meer wil gaan patrouilleren op het internet om elke vorm van computercriminaliteit te bestrijden, van fraude en terrorisme tot cyberpedofilie. Momenteel werken reeds 145 mensen op de computereenheid van de Federale Politie en die hebben hun handen vol.

Ook Tom Van Renterghem van Child Focus doet zijn inbreng in de reportage. Hij organiseert informatieavonden voor zowel kinderen als ouders. De heer Van Renterghem dringt er vooral op aan dat ouders met hun kinderen moeten praten over het internetgebruik en dat ze samen met hen een vergelijking moeten maken met de reële wereld: je gaat toch ook niet in je blootje in een bomvolle winkelstraat staan, …

Een reporter van Panorama ging zelf voor de chatbox zitten en deed zich voor als een dertienjarig meisje. Hij kwam al snel in aanraking met cyberpedofielen. Een actrice, Sophie, werd ingehuurd om af te spreken met de betrokken mannen. Een verborgen camera registreerde alles.

Eerst sprak Sophie af met een man die ze leerde kennen via een chatbox. Ze spraken af in het café van het Centraal Station van Antwerpen. De man wou samen met haar een lingeriesetje kopen voor haar verjaardag en vroeg haar of ze dat dan ook ging aantrekken. De man stuurde aan op seks, maar vertelde haar dat hij niet tot het uiterste wou gaan. Maar wat is het uiterste? …

Een andere situatie: Sophie vindt op een website een zoekertje van een man die 300 euro aanbood voor een meisje dat één à twee uur zichzelf naakt wou laten filmen. De actrice Sophie sprak met die man af en vroeg hem over de zaken die hij haar in het filmpje wou laten doen. Hij vertelde haar dat het filmen zou gebeuren in zijn eigen huis wanneer zijn vrouw gaan werken was. Volgens de man zou het filmpje gebruikt worden voor eigen gebruik en eventueel ook om door te sturen naar hele goeie vrienden van hem. Ook bleek hij maar weinig moeite te hebben met het feit dat Sophie nog zo jong was en dat ze nog geen of maar weinig ervaring had. Als deze man seks zou hebben met een veertienjarige en dat zou filmen, dan kan hij veroordeeld worden voor verkrachting en aanmaak van kinderporno. Die feiten moeten dan wel eerst aan het licht komen, want de politie treedt meestal pas in werking wanneer iemand aangifte doet of als er een melding komt bij de Federal Computer Crime Unit.

Sophie kwam via een chatbox ook nog in contact met een andere man, die al gauw erg dominant te werk ging. De man zei dat hij haar een computervirus had doorgestuurd die al haar bestanden zou wissen vanaf het moment dat ze de computer terug zou opstarten. Als Sophie goed meewerkte en hem een topless foto zou doorsturen, zou hij het computervirus misschien nog kunnen tegenhouden.

Er kan geconcludeerd worden dat de slachtoffers van cyberpedofielen meestal meisjes zijn tussen dertien en vijftien jaar. Vaak gaat het over meisjes die gepest worden, een negatief zelfbeeld hebben en op zoek zijn naar aandacht. De slachtoffers van cyberpedofielen (en van traditionele pedofielen) worden steeds jonger. Als we kijken naar de traditionele pedofielen, dan zien we dat zelfs weerloze baby's gepenetreerd worden; kijken we naar cyberpedofilie, dan zien we dat handige zesjarigen al het slachtoffer zijn (in België is zo'n geval bekend). Ook de taferelen worden steeds gewelddadiger: kinderen die vastgebonden worden, kinderen die seks met dieren moeten hebben, …

Dit is een interessante reportage, die inzicht geeft in de wereld van de cyberpedofilie. De reportage geeft een ruim en overzichtelijk beeld waarin getuigenissen zitten van Vlaamse jongeren. Als u dacht dat cyberpedofilie een ver-van-uw-bed-show was, dan zet deze reportage u met beide voeten terug op de grond.

Hieronder ziet u de aankondiging van de reportage uit het Nieuwsblad van zondag 4 maart 2007.

„Geschokt dat het zo snel ging"

PANORAMA: KINDERLOKKERS ONLINE
CANVAS • 20 UUR

In *Kinderlokkers online* zoekt Panorama uit hoe pedofielen via het internet contacten leggen. Het aas waarmee journalist Johan Ghysens een cyberpedofiel wist te strikken, heet 'Lotte', een fictief meisje van dertien.

Cathérine De Kock

Journalist Johan Ghysens schuimde met zijn fictief alter ego 'Lotte' chatrooms en datingsites voor jongeren af. Hij komt er al snel de cyberpedofiel 'Beertje' tegen, een man van 34 die met 'Lotte' wil afspreken en liefst nog meer dan dat alleen.

Hoe slaag je er als volwassen man in om je als een meisje van 13 voor te doen?

„Ik heb al gelijkaardige reportages gemaakt voor *Koppen*, onder meer over cyberpesten bij tieners. Tijdens die reportage viel me het expliciete taalgebruik tussen tieners op. Daarnaast heb ik me geïnspireerd op profielsites voor jongeren, zoals RedBox. Daar plaatsen tieners hun foto en details over zichzelf op. Het is zowat hun uithangbord op het internet."

Hoe was het voor u om te weten dat u aan het chatten was met een pedofiel?

„Ik had al gelezen over pedofielen op het internet, maar dacht nooit dat er zo snel reactie zou komen op mijn profiel. Amper twintig minuten nadat ik mijn profiel had aangemaakt, stuurde 'Beertje' me al een berichtje met de vraag of ik met hem wou chatten. Als je nadien beseft dat hij een man van 34 is die seks wou met 'Lotte', dan schrik je. Ik was echt geschokt dat het zo snel was gegaan."

Probeerde hij zijn leeftijd niet geheim te houden?

„Nee. Zijn foto stond bij zijn profiel: je zag meteen dat hij een oudere man was. Hij speelde zelfs in op het feit dat hij ouder was en Lotte jonger. Hij zei me bijvoorbeeld dat ik moest oppassen met al die oudere mannen die met mij zouden willen chatten, waarmee hij duidelijk wou maken dat hij net wél te vertrouwen was."

„Het eerste chatgesprek met 'Beertje' ging over koetjes en kalfjes en zijn stukgelopen relatie. Maar tijdens het tweede chatgesprek begon hij al over seks en probeerde bij 'Lotte' zo ver te krijgen dat ook zij seksueel getinte dingen vertelde. Hij heeft toen ook voorgesteld om af te spreken. Hij wou 'Lotte' lingerie kopen voor haar verjaardag en drong ook aan om dan samen in het pashokje te kruipen."

„Als je nadien beseft dat een man van 34 seks wou met een meisje van 13, dan schrik je"
Johan Ghysens, reporter

En?

„We hebben een meerderjarige actrice met een erg jong uiterlijk naar die ontmoeting gestuurd. We hadden afgesproken dat ze een aantal dingen te weten moest komen. Toen ze daarmee klaar was, heeft ze 'Beertje' wijsgemaakt dat haar vader haar woedend had opgebeld met de vraag om meteen naar huis te gaan. Zijn ogen spraken boekdelen op het moment, heel angstig en geconcentreerd. Hij bleef aandringen om haar lingerie te kopen en probeerde haar ook te kussen."

Wat gebeurde er na die ontmoeting? Bleef hij 'Lotte' lastigvallen?

„Hij heeft nog enkele berichtjes gestuurd met de vraag om elkaar nogmaals te ontmoeten. Voor ik al-

le contact verbrak, volgde er ook nog een chatgesprek. Hij zei steeds dat hij met 'Lotte' niet tot het uiterste zou gaan. Toen ik vroeg wat hij daarmee bedoelde, zei hij: 'Neuken doe ik niet, maar misschien wel in uw konijn'."

Weet 'Beertje' ondertussen dat Lotte eigenlijk geen meisje van 13 is en dat hij nu figureert in een undercoverreportage?

„Nee, hij weet nog steeds van niets. Hij werd sowieso onherkenbaar gemaakt."

Heeft u zijn gegevens doorgespeeld aan het gerecht?

„Nee, want in principe zijn er geen strafbare feiten gepleegd. Het undercovermeisje is immers meerderjarig. Maar als de politie erom vraagt, dan zijn we deontologisch verplicht om die informatie vrij te geven."

1 De 34-jarige pedofiel probeert het undercovermeisje te kussen.

2 Tijdens het tweede chatgesprek al begon de pedofiel expliciet over seks. ©vrt

Kinderlokkers van toen op het internet

Programma: Netwerk
Zender: Nederland 2
Uitzenddatum: 9 maart 2007
Duur: 21 minuten en 43 seconden
Titel van de uitzending op dvd:
'Netwerk – Kinderlokkers online 09/03/2007'

Deze Netwerk-uitzending is een verkorte versie van de reportage die Panorama maakte over cyberpedofielen (uitzenddatum 4 maart 2007). Netwerk zorgt wel voor een eigen inleiding en slot.

De troebele wereld van kindermisbruik via het internet

Programma: Koppen
Zender: Één
Uitzenddatum: 5 juni 2007
Duur: 30 minuten en 11 seconden
Titel van de uitzending op dvd:
'Koppen – Kinderlokkers online 05/06/2007'

Deze Koppen-uitzending is een verkorte versie van de reportage die Panorama maakte over cyberpedofielen (uitzenddatum 4 maart 2007).

2.4 Cyberpesten

Pestgedrag dat gebeurt in cyberspace ⇨ cyberpesten

Programma: Koppen
Zender: Één
Uitzenddatum: 16 maart 2006
Duur: 11 minuten en 19 seconden
Titel van de uitzending op dvd:
'Koppen – Cyberpesten 16/03/2006'

Een reportage over cyberpesten. Het Vlaams Instituut voor Wetenschappelijk en Technologisch Aspectenonderzoek voerde samen met de Universiteit van Antwerpen een onderzoek uit naar cyberpesten bij Vlaamse jongeren. Koppen kreeg als eerste de kans om deze onderzoeksresultaten in te kijken en dit was tevens de aanleiding voor het tot stand komen van deze reportage.

In de reportage ziet u een jonge tiener, Veerle Peeters, die al een jaar gepest wordt zowel op school als op het internet. De pesterijen begonnen toen Veerle een MSN-gesprek voerde met een goede vriend van haar. Die vriend vroeg of ze haar borsten wilde tonen voor de webcam. Toen ze dat weigerde, begon hij haar uit te schelden. Veerle Peeters ging uiteindelijk toch op zijn verzoek in en hij kreeg haar zelfs zover dat ze al haar kleren uittrok. Hij nam foto's van die webcambeelden en stuurde ze door naar een vriend die ze dan weer doorstuurde naar verschillende anderen. In 1, 2, 3 had de helft van Veerle's school de foto's die avond nog gezien. Er werd ook een website gemaakt in Veerles naam met die bewuste foto's. Veerle en haar ouders klopten bij de lokale politie aan en de dader riskeert een straf voor het versturen van haatmail en publiceren van foto's zonder toestemming.

Een ander meisje, dat voor Koppen getuigde, is Jolien Van der Steen. Zij wordt al een tijdje gepest omdat iemand met haar e-mailadres een e-mail met vunzige praat verstuurde naar alle leerlingen van de school. De politie werd ingeschakeld, maar vond de dader niet. Uiteindelijk is door een medeleerling van Jolien de dader aan het licht gekomen. Blijkbaar had een vriend van Jolien uit verveling haar e-mailadres gekraakt en die e-mail verstuurd met alle gevolgen vandien.

In de reportage komt ook Vlaams volksvertegenwoordiger Jan Roegiers (Spirit) aan het woord, die wat algemene uitleg geeft over cyberpesten.

Pestgedrag dat gebeurt in cyberspace ⇨ cyberpesten

Programma: De Zevende Dag
Zender: Één
Uitzenddatum: 26 maart 2006
Duur: 12 minuten en 30 seconden
Titel van de uitzending op dvd:
'De Zevende Dag – Cyberpesten 26/03/2006'

In het programma De Zevende Dag wordt een gesprek gevoerd met:

- Steven Goegebuer, leraar en een schrijver van een interactief theaterstuk over cyberpesten;
- Marianne Bogaert, directrice van het EVO (Educatieve Vereniging voor Ouderwerking in het officieel onderwijs);
- Lief De Meester, moeder van een slachtoffer van cyberpesten.

In het gesprek wordt duidelijk wat cyberpesten is en er worden hiervan ook enkele voorbeelden gegeven. Verder wordt er over een aantal zaken rond cyberpesten gepraat, zoals wie de slachtoffers en daders zijn, wat de gevolgen van cyberpesten kunnen zijn, enkele tips, …

Wat vooral uit het gesprek kan opgemaakt worden, is dat de ouders en de school goed moeten samenwerken – nog meer dan bij het traditionele pesten - om cyberpesten te voorkomen en te bestrijden.

Eekloose Happy Slapping?!

Programma: Het Journaal
Zender: Één
Uitzenddatum: 29 september 2006
Duur: 1 minuut en 30 seconden
Titel van de uitzending op dvd:
'Journaal – Happy Slapping 29/09/2006'

Het nieuwsbericht gaat over een school in Eeklo waar een gevecht werd gefilmd met de gsm en waarbij het betreffende filmpje op het internet belandde. Persoonlijk zou ik denken dat dit een geval is van happy slapping, maar de school en de politie ontkent dit. Zij vinden dat ze in Eeklo nog niet te maken hebben met dergelijke Amerikaanse toestanden. Diegene (tot nu toe onbekend) die het filmpje op het internet plaatste, riskeert een sanctie omdat hij het schoolreglement overtrad dat filmen op school verbiedt.

2.5 Second Life

Second Life, een tweede leven in drie dimensies op het internet

Programma: Panorama
Zender: Canvas
Uitzenddatum: 15 juli 2007
Duur: 44 minuten en 16 seconden
Titel van de uitzending op dvd:
'Panorama – Second Life 15/07/2007'

Deze Panorama-uitzending gaat over Second Life, een virtuele wereld. In België is Second Life nog niet zo populair als in de rest van de wereld. Toch wil Panorama u een kijkje gunnen in de virtuele wereld. Een wereld waar 45 % van de avatars vrouwen zijn, elk moment ongeveer 20 000 mensen ingelogd zijn (er is dus altijd wel iemand aanwezig) en een wereld waar de verbeelding geen grenzen kent.

In de reportage komen mensen aan het woord, die uitleg geven over het ontstaan van Second Life, de bewoners ervan, … We krijgen zowel voor- als tegenstanders van Second Life te zien:

- Philip Rosedale, CEO van Linden Lab;
- Chris Collins, commercieel analist bij Linden Lab;
- Ailin Graef, een steenrijke projectontwikkelaar die virtueel in Second Life actief is;
- Kevin Kelly, medeoprichter van Wired Magazine;
- Veronica Brown, virtueel modeontwerpster;
- Lauren Gelman van de Stanford University;

- Peter Yellowlees van de University of California;
- Ted Castronova, professor telecommunicatie;
- Clay Shirky;
- Luke Connell van World Stock Exchange;
- Julian Dibbell, auteur van Play Money;
- Bill Gurley;
- Brad Kasell van Emerging Technologies – IBM;
- Dan Miller, fiscaal adviseur.

Virtuele kinderporno moet verboden worden

Programma: Het Nieuws
Zender: VTM
Uitzenddatum: 23 maart 2007
Duur: 2 minuten en 8 seconden
Titel van de uitzending op dvd:
'Het Nieuws – Virtuele kinderpornografie in SL 23/03/2007'

Een nieuwsbericht over virtuele kinderpornografie zoals in het spel Second Life. Volgens Stefanie Anseeuw (senator Open VLD) moet ook virtuele kinderpornografie op het internet bestraft worden. Uit onderzoek blijkt dat mensen, die op het internet virtuele seks (willen) beleven met kinderen, dit ook in de echte wereld willen.

Volgens de Belgische wetgeving is kinderporno bekijken op zich niet strafbaar, maar het bewust verspreiden en bewaren van kinderporno wel. Het hoeft daarbij niet te gaan om echte kinderen. De bezitter van afbeeldingen van seksuele handelingen, waarin een minderjarige wordt voorgesteld, is strafbaar. Deze minderjarige hoeft geen reële persoon te zijn, het kan bijvoorbeeld ook een avatar zijn. Het is onmogelijk dat enkel België virtuele kinderporno probeert aan banden te leggen. Europa kan echter wel aandringen dat de makers van virtuele spelen, zoals Second Life, beperkingen opleggen. Zo zouden ze bijvoorbeeld kunnen instellen dat een persoon geen seks kan hebben met een afbeelding van een kind. Gelukkig zijn er in België nog geen klachten geweest omtrent virtuele kinderporno. Men kan beter voorkomen dan genezen.

2.6 Internetverslaving

Internetverslaving: de verleiding van het wereldwijde web

Programma: Netwerk
Zender: Nederland 2
Uitzenddatum: 16 maart 2007
Duur: 10 minuten
Titel van de uitzending op dvd:
'Netwerk – Internetverslaving 16/03/2007'

Een Nederlandse reportage over internetverslaving. Bijna elk Nederlands gezin heeft internet. 94 % van hen beschikt over een breedbandverbinding. Al gauw is de kans op internetverslaving groot en vooral jongeren zijn hier gevoelig voor. Andere zaken zoals schoolwerk moeten wijken voor hun internetverslaving.

Uit onderzoek blijkt dat minstens dertigduizend Nederlandse jongeren verslaafd zijn aan het internet. Ze zijn verslaafd aan internetporno, chatten en/of internetgames. Nederlandse jongeren raken vooral verslaafd aan internetgames zoals World Of Warcraft, een vechtspel dat nooit uitgespeeld kan worden, waardoor het moeilijk is om ermee te stoppen. Pokeren is tegenwoordig de nieuwe hype en ook het internetpokeren via illegale websites ligt tegenwoordig goed in de markt. De internetverslaving wordt deels in de hand gewerkt doordat 43 % van de Nederlandse jongeren een computer met internet op hun eigen kamer hebben, zodat ze meer ruimte en privacy hebben om te doen wat ze willen.

In de reportage komen enkele mensen aan het woord

- Tom (fictieve naam), een internetverslaafde;
- Monique (fictieve naam), moeder van de internetverslaafde Tom;
- Regina van den Eijnden van het onderzoeksbureau IVO die het internetgebruik onder jongeren in kaart bracht via een enquête onder 50 000 Nederlandse tieners;
- Albert Benschop, internetsocioloog;
- Arda Gerkens, Tweede Kamer SP;
- André Rouvoet, de nieuwe Nederlandse Minister van Jeugd en Gezin; hij maakt zich al een tijdje zorgen over de gevaren op het internet.

Om de reportage af te sluiten wordt gemeld dat een zesentwintigjarige Chinees om het leven is gekomen omdat hij zeven dagen zonder onderbreking deelnam aan een internetspel.

3 Campagnes

Af en toe vindt er een campagne plaats rond de gevaren van het internet. Deze reclamecampagnes kunnen gericht zijn op ouders, jongeren, leerkrachten… Soms is het handig en raadzaam om bijvoorbeeld in een klassituatie in te spelen op die campagnes.

3.1 Campagnefilmpjes

Af en toe ziet u in de reclame van een of andere tv-zender of op het internet een campagnefilmpje voor een veiliger internet. Hieronder vindt u een opsomming van enkele mooie campagnefilmpjes.

	Het Nederlandse SIRE maakte een aangrijpend campagnefilmpje rond cyberpesten. Het filmpje doet een oproep aan ouders om te controleren wat hun kinderen op het internet doen en om cyberpesten mee te helpen bestrijden. Het campagnefilmpje is te bekijken op YouTube onder de naam 'digitaal pesten' (http://nl.youtube.com/watch?v=25dZjMQzjeg)
	Het campagnefilmpje 'Dating show' is ontstaan door het Nederlandse DIGIbewust. De bedoeling ervan is jongeren duidelijk te maken dat ze hun wachtwoord niet mogen doorgeven. Het campagnefilmpje is te downloaden via http://www.digibewust.nl en is ook te vinden op de dvd ingesloten in de eindwerkdoos (Campagnefilmpje DIGIbewust - Datingshow.wmv)
	Het campagnefilmpje 'Zinnetjes' is ontstaan door het Nederlandse DIGIbewust. De bedoeling ervan is jongeren duidelijk te maken dat ze een veilig en complex wachtwoord moeten vormen Het campagnefilmpje is te downloaden via http://www.digibewust.nl en is ook te vinden op de dvd ingesloten in de eindwerkdoos (Campagnefilmpje DIGIbewust - Zinnetjes.wmv)
	Het campagnefilmpje 'Waar is Chris' is van oorsprong een Duits filmpje, maar werd in het Nederlands beschikbaar gesteld door DIGIbewust. De bedoeling van dit campagnefilmpje is ouders bewust te maken dat ze hun kinderen moeten beschermen op het internet. Het campagnefilmpje is te downloaden via http://www.digibewust.nl en is ook te vinden op de dvd ingesloten in de eindwerkdoos (Campagnefilmpje DIGIbewust – Waar is Chris.wmv)

3.2 Preventieaffiche: Click Safe

Click Safe is een Belgische organisatie die zich inzet voor een veiliger internet. Op hun website kunt u onder andere tips vinden voor zowel kinderen, jongeren, ouders en leerkrachten.

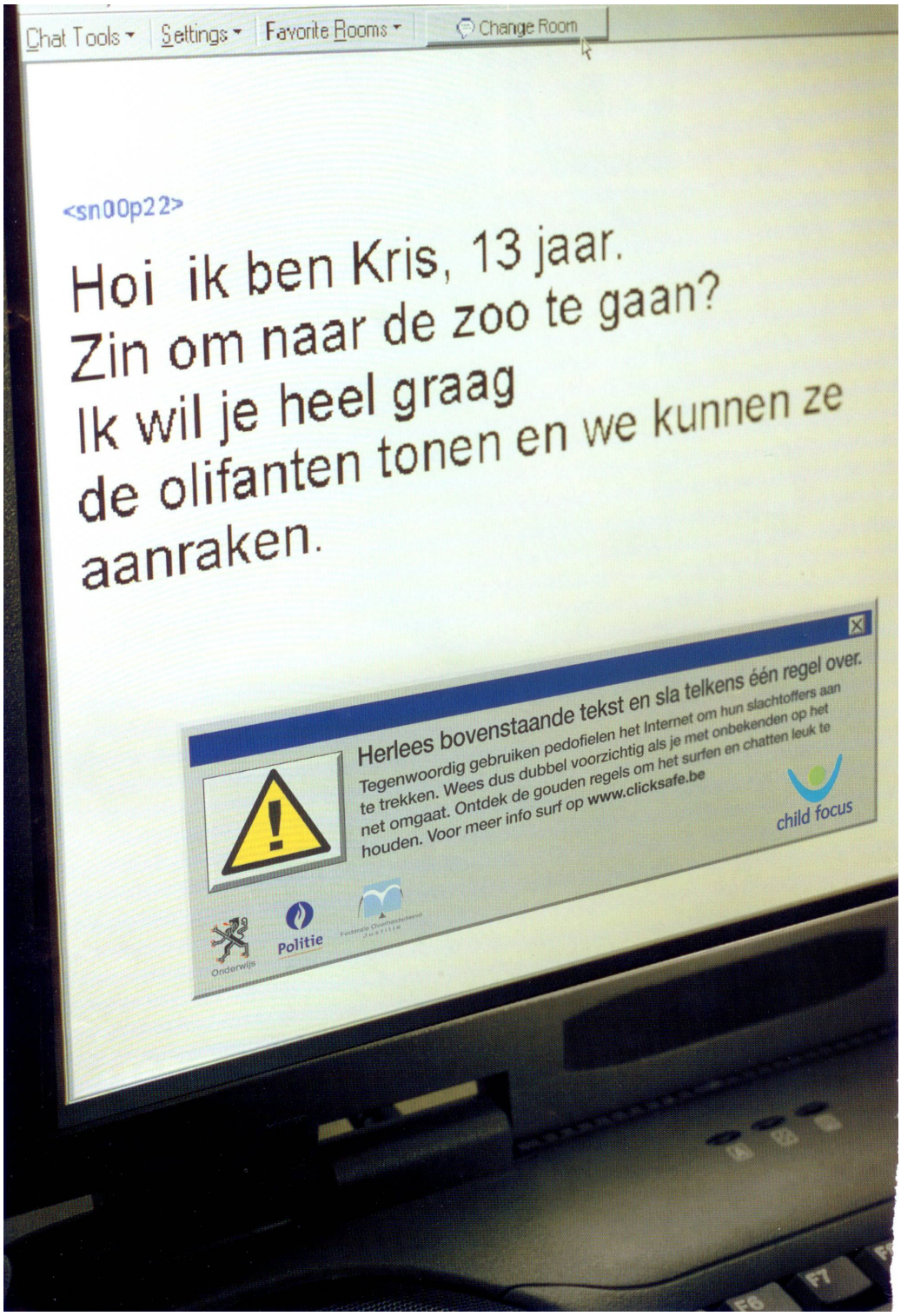
Onderstaande affiche met tips is een aanrader om in het klaslokaal te hangen en kinderen en/of jongeren op deze tips te wijzen.

3.3 Campagne Child Focus

Child Focus, het Europees Centrum voor Vermiste en Seksueel Uitgebuite Kinderen, organiseert of werkt vaak mee aan campagnes voor veiliger internet.

In 2003 publiceerden zij in samenwerking met nog enkele andere instanties (bijvoorbeeld Vlaams Ministerie van Onderwijs en Vorming) onderstaande affiche. Hierop wordt duidelijk gemaakt dat niet iedereen op een chatbox even goede bedoelingen heeft en dat ook pedofielen op chatboxen vertoeven. De affiche verscheen in enkele magazines.

Deze affiche vond ik terug in het jongerenmagazine ID van januari 2003.



3.4 Als een visje door het net

'Als een visje door het net' is een Belgische jongerengids over slim en veilig surfen. Het boekje werd samengesteld door Microsoft, ChildFocus en de Federal Computer Crime Unit (FCCU). Het boekje is vooral gericht naar jongeren tussen tien en veertien jaar.

Begin september werden honderdduizend exemplaren van dit boekje verspreid via Het Nieuwsblad op Zondag. In bijlage vindt u de digitale versie van het boekje (http://ond.vvkso-ict.com/vvksosites/item.asp?WID=35&PID=2654)

3.5 Ginette – Hoe ik mijn peeceefobie overwon

In het boekje 'Hoe ik mijn peeceefobie overwon' geeft Ginette tips over veilig computeren en internetten. Het boekje is vooral gericht aan volwassen computerleken, maar het is voor iedereen leuk en interessant om het eens te doorbladeren.

Het boekje ligt goed in de hand en telt slechts 29 pagina's. Het werd gesponsord door verschillende organisaties, maar is hoofdzakelijk een initiatief van het project 'Internet voor iedereen'.

'Hoe ik mijn peeceefobie overwon' kunt u gratis verkrijgen in enkele winkels (vooral computerwinkels) en via de website http://www.peeceefobie.be. Jammer genoeg zijn deze boekjes niet meer beschikbaar. In de eindwerkdoos zit wel nog een boekje voor u ingesloten.

Peeceefobie van start

Veiligheidscampagne voor iedereen

Samen met de bedrijfswereld heeft minister Vanvelthoven *Peeceefobie* opgestart, een informatiecampagne rond het veilig gebruik van de computer en het internet. Er komen zeven thema's aan bod: beveiliging van computers, gebruik van wachtwoorden, omgaan met e-mail van onbekenden, beschermen van persoonlijke gegevens, veilig uitvoeren van financiële transacties, oppassen met downloaden en waakzaamheid.

Vanvelthoven merkt aan de hand van een enquête op dat ruim een derde van de Belgen dagelijks surft en zegt het internet niet meer te kunnen missen. Aan de andere kant wil meer dan een kwart van de mensen geen aankopen doen via het web uit wantrouwen of schrik. Sterker is dat uit dit onderzoek blijkt dat minder dan de helft van de pc-bezitters antivirussoftware gebruikt en slechts een kwart een firewall heeft of zich tegen spam en spyware beschermt. En al even alarmerend: meer dan de helft heeft nog nooit van spyware en firewalls gehoord. Een derde weet niet wat antivirussoftware is.

Met de campagne wil Vanvelthoven zoveel mogelijk mensen op de digitale trein laten springen, maar niet zonder tekst en uitleg. Het personage *Ginette* speelt daarin de hoofd-rol. Zij is *peeceefoob* en houdt niet van computers en het internet. Ze vindt het gevaarlijk en ingewikkeld. Toch gaat ze op een dag door de knieën. In haar eigen woorden legt ze uit wat jij er volgens haar ook over moet weten. De peeceefobiewebsite bevat alle uitleg over de zeven veiligheidstips, en diagnosegereedschap, waarmee je kunt achterhalen hoe veilig of onveilig je internet.

■ www.peeceefobie.be

Bron: Netwerk (december 2005)

3.6 Diploma Veilig Internet

'Diploma Veilig Internet' is een lespakket, dat vooral gericht is aan kinderen van de laatste graad basisonderwijs. Het lespakket informeert kinderen over hoe ze veilig het internet op kunnen. Na afloop van de lessen, kunnen de kinderen zelfs een diploma voor veilig internetgebruik krijgen.

Ik heb het lespakket aangevraagd en vind het zeer interessant en kindvriendelijk: een aanrader voor het basisonderwijs.

Leerkrachten kunnen het lespakket gratis aanvragen via www.diplomaveiliginternet.nl.

3.7 Brochure 'Hoe digibewust bent u?'

In de brochure 'Hoe digibewust bent u?' krijgt u uitleg over enkele toepassingen van het internet en komt u meer te weten over enkele internetgevaren zoals chatten, onveilig internetbankieren, …

De brochure is voor een volwassen doelpubliek. Er staan tips in hoe u uw computer, uzelf en uw kinderen kunt beschermen op het internet.

De brochure kunt u voorlopig nog downloaden via http://www.digibewust.nl, maar ze zit ook verwerkt in de bijlagen.

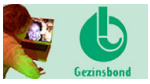
3.8 Suske en Wiske-album 'De Sinistere Site'

Minister van Werk en Informatisering Peter Vanvelthoven kwam op het idee om een Suske en Wiske-album uit te brengen, om kinderen ervan bewust te maken dat er ook gevaren op het internet schuilen. Samen met Child Focus en Studio Vandersteen werd deze realisatie tot stand gebracht. Het album werd verdeeld in Nederlandstalige en Franstalige basisscholen. Ook Nederland verdeelt in oktober de strips in enkele Nederlandse basisscholen.

Achteraan in het Suske en Wiske-album zijn enkele nuttige tips te vinden voor veilig chatten en veilig e-mailen en surfen. Ik heb het stripalbum gelezen en vind het geschikt voor het vierde, vijfde en zesde leerjaar van het basisonderwijs. 'De Sinistere Site' maakt kinderen alert dat er internetgevaren zijn, maar correcte uitleg over wat dit precies inhoudt, kunt u er niet vinden. De boodschap die het Suske en Wiske-album meegeeft is dat het internet niet zonder gevaren zit en dat u moet opletten welke persoonlijke gegevens u op het internet zet.

Als u nog een exemplaar van dit album wilt bemachtigen, dan zult u een rondvraag moeten doen, want jammer genoeg is het stripalbum niet meer te verkrijgen via de reguliere manier in België en Nederland.

3.9 Website Veilig Online



Nog niet zo lang geleden lanceerde de Gezinsbond in samenwerking met Child Focus een website voor ouders over veilig internet. Op de website kunt u onder andere tips en situatiefilmpjes vinden over hoe te reageren bij vaststelling van onzedelijk gedrag op de computer. U vindt de website op volgend internetadres: http://www.gezinsbond.be/veiligonline

Natuurlijk zijn er nog tal van andere interessante websites rond veilig internet die u kunt bezoeken, maar de situatiefilmpjes op de website van de Gezinsbond zijn voor ouders zeker het bekijken waard.

Website voor veilig kinderinternet

De Gezinsbond en Child Focus hebben een website gemaakt over veilig internetgebruik door kinderen. De bedoeling van de website is te voorkomen dat kinderen op pornosites surfen of in een chatbox contact krijgen met een pedofiel.
Op de site staan opvoedingstips, adviezen om de computer veilig in te stellen en beelden over kinderen die onveilig chatten, mailen en surfen.
'We laten bijvoorbeeld zien hoe een chatbox veilig kan worden ingesteld zodat uw kind alleen maar kan chatten met de personen die je zelf wil en dat maar een beperkt aantal personen kan zien dat uw kind online is', zegt Michaël Op de Beeck van de Gezinsbond.
De website 'Onze kinderen veilig online' is bereikbaar via www.gezinsbond.be en www.childfocus.org. (belga)

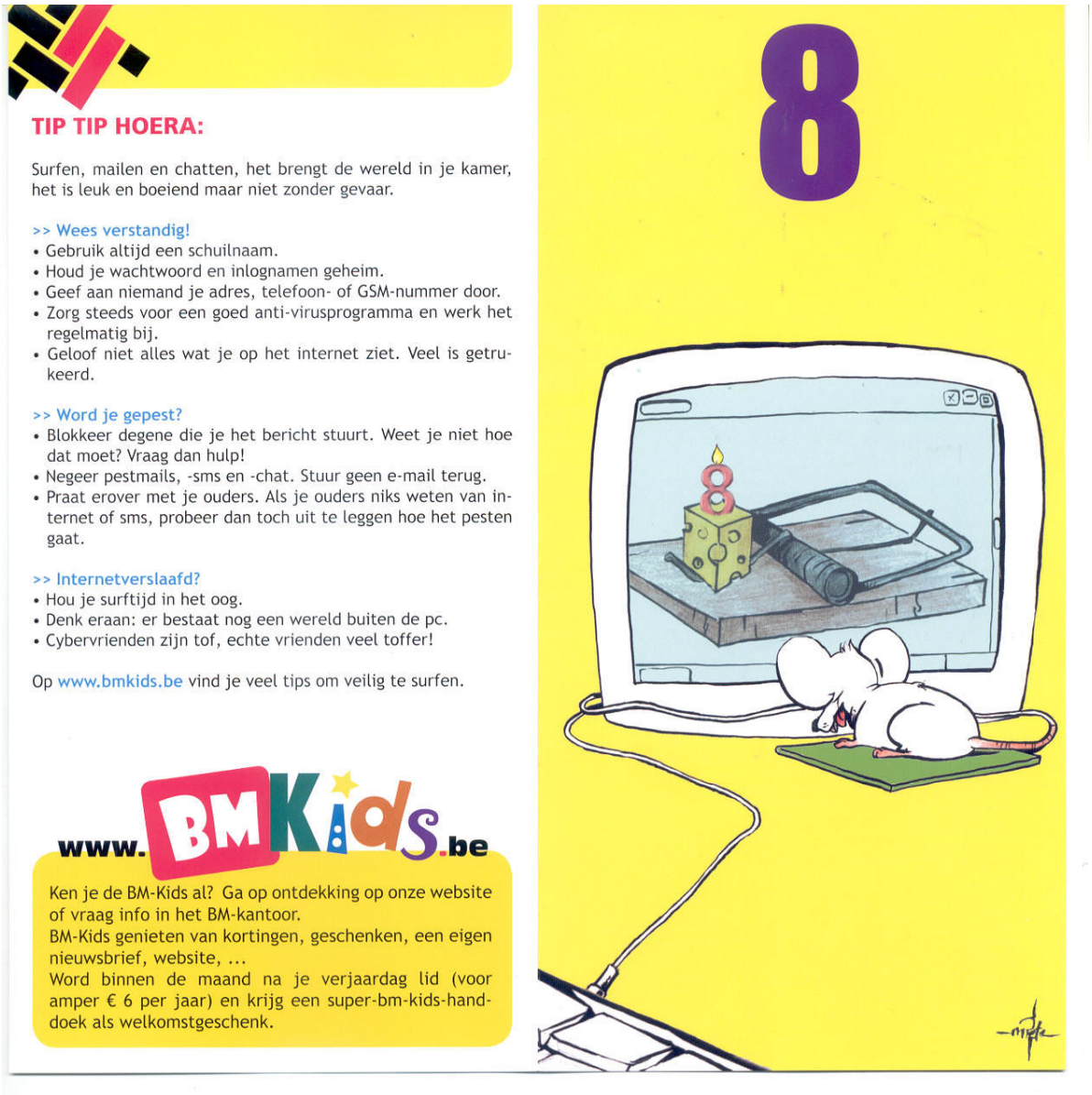
Bron: Het Nieuwsblad (29 juni 2007)

3.10 Verjaardagskaart

Het Ziekenfonds Bond Moyson stuurt naar alle achtjarige leden een verjaardagskaart, die hen bewust maakt van internetgevaren (onder andere cyberpesten). Een leuk initiatief.

De voorzijde van de verjaardagskaart:

De keerzijde van de verjaardagskaart:



TIP TIP HOERA:

Surfen, mailen en chatten, het brengt de wereld in je kamer, het is leuk en boeiend maar niet zonder gevaar.

>> Wees verstandig!
- Gebruik altijd een schuilnaam.
- Houd je wachtwoord en inlognamen geheim.
- Geef aan niemand je adres, telefoon- of GSM-nummer door.
- Zorg steeds voor een goed anti-virusprogramma en werk het regelmatig bij.
- Geloof niet alles wat je op het internet ziet. Veel is getrukeerd.

>> Word je gepest?
- Blokkeer degene die je het bericht stuurt. Weet je niet hoe dat moet? Vraag dan hulp!
- Negeer pestmails, -sms en -chat. Stuur geen e-mail terug.
- Praat erover met je ouders. Als je ouders niks weten van internet of sms, probeer dan toch uit te leggen hoe het pesten gaat.

>> Internetverslaafd?
- Hou je surftijd in het oog.
- Denk eraan: er bestaat nog een wereld buiten de pc.
- Cybervrienden zijn tof, echte vrienden veel toffer!

Op www.bmkids.be vind je veel tips om veilig te surfen.

www.BMKids.be

Ken je de BM-Kids al? Ga op ontdekking op onze website of vraag info in het BM-kantoor.
BM-Kids genieten van kortingen, geschenken, een eigen nieuwsbrief, website, ...
Word binnen de maand na je verjaardag lid (voor amper € 6 per jaar) en krijg een super-bm-kids-handdoek als welkomstgeschenk.

8

4 Artikels

Tijdens mijn lerarenopleiding heb ik in functie van mijn eindwerk de actualiteit gevolgd. Ik heb een artikelenbundel samengesteld met een greep uit de interessantste en leerrijkste artikels over internetgevaren die de laatste jaren verschenen zijn. Een aanrader om ze eens door te nemen, want niet alle informatie die u er terugvindt, werd opgenomen in het theoretische gedeelte van mijn eindwerk. U kunt de artikelenbundel terugvinden in de eindwerkdoos.

Ik wens u alvast veel leesplezier!

5 Multimedia dvd

Toen ik het onderwerp van mijn eindwerk koos, was ik vast besloten om ook iets praktisch rond dit thema te doen. Iets wat later nog door mezelf of door anderen gebruikt kon worden. Na overleg met enkele leerkrachten uit het secundair onderwijs stelde ik vast dat er een grote nood is aan goed lesmateriaal rond het thema internetgevaren. In enkele informaticaboeken staat hierover wel iets vermeld, maar dit is echter niet voldoende.

Naar mijn gevoel spreekt een infobundel en/of cursus over internetgevaren, jongeren niet voldoende aan. Ik kwam daarom al snel op het idee om een multimedia dvd te maken. Deze is vooral gericht tot jongeren van de tweede graad, maar kan ook volwassenen interesseren die wat meer kennis willen opdoen over vaak voorkomende internetgevaren.

In de multimedia dvd zijn af en toe ook 'grote' stukken tekst te vinden, maar die zijn broodnodig om de jongeren voldoende te informeren. Elk thema, met uitzondering van cyberpesten, wordt afgesloten met één of twee oefeningen. Via deze oefeningen kan kort getest worden of alle informatie wel goed doorgenomen werd en het is tevens een uitstekende manier om nog eens enkele belangrijke zaken op te frissen.

Aangezien beelden soms meer vertellen dan woorden zijn er twee thema's voorzien van een filmpje. Het zijn interessante fragmenten uit reportages, die ik het geschiktst en aangrijpendst vond voor jongeren. Op het einde van elk filmpje wordt de bron vermeld.
Bij het onderdeel onveilig chatten leert een eigen gemaakt filmpje hoe je een contactpersoon in de gesloten chatbox MSN blokkeert en deblokkeert. Onder het besturingssysteem Windows XP vormt het bekijken van dit filmpje geen enkel probleem. Windows Vista daarentegen kan hiervoor mogelijks een codec vragen.

De multimedia dvd is een website die gemaakt werd met het programma Dreamweaver CS3 en op een cd-rom werd gebrand die automatisch wordt opgestart. Deze website is ideaal om in lessen te gebruiken. Daarom opteerde ik om de website (voorlopig) niet online te plaatsen en hem als multimedia dvd te benoemen. In een klasgebeuren kan het thema internetgevaren 'ingekaderd' worden en kunnen de leerkrachten de leerlingen ook ondersteunen bij eventuele reacties, problemen, getuigenissen, … Deze multimedia dvd kan ook ingeleid en/of samen gebruikt worden met andere zaken rond dit thema zoals campagnes, een film, … Meer informatie over dergelijke bewustmakingsmiddelen heeft u normaal gezien al doorlopen in de voorgaande hoofdstukken van dit deel. In een lessituatie kan men er bijvoorbeeld voor opteren om telkens één deel van het thema internetgevaren (bijvoorbeeld het deel computervirussen) per twee lesuren onder handen te nemen.

Doorheen de multimedia dvd (website) navigeren is heel eenvoudig. Onder de titel 'De grootste internetgevaren voor jongeren' is er een horizontale balk met hyperlinks naar de verschillende delen (bijvoorbeeld hackers, spyware, …). Als je op een dergelijke hyperlink klikt, dan verschijnt het eerste hoofdstuk van dat deel. Aan de rechterkant van het venster komen tegelijkertijd hyperlinks die je doorverwijzen naar de andere hoofdstukken van dat deel. In feite spreekt de navigatie doorheen de multimedia dvd voor zich.

Volgende delen zijn verwerkt in de dvd-r:
- home (inleiding);
- computervirussen;
- spam;
- hackers;
- spyware;
- onveilig chatten;
- cyberpesten.

Hieronder volgt per deel van de website een korte opsomming van de verschillende hoofdstukken. Per deel vindt u ook de oplossingen van de oefeningen. In principe kan ik hieron-

der de volledige multimedia dvd beschrijven, maar ik ben ervan overtuigd dat u meer bijleert wanneer u er zelf doorheen navigeert en dus zelf de teksten, pdf-documenten, filmpjes, … ontdekt.

Veel ontdekkingsplezier!

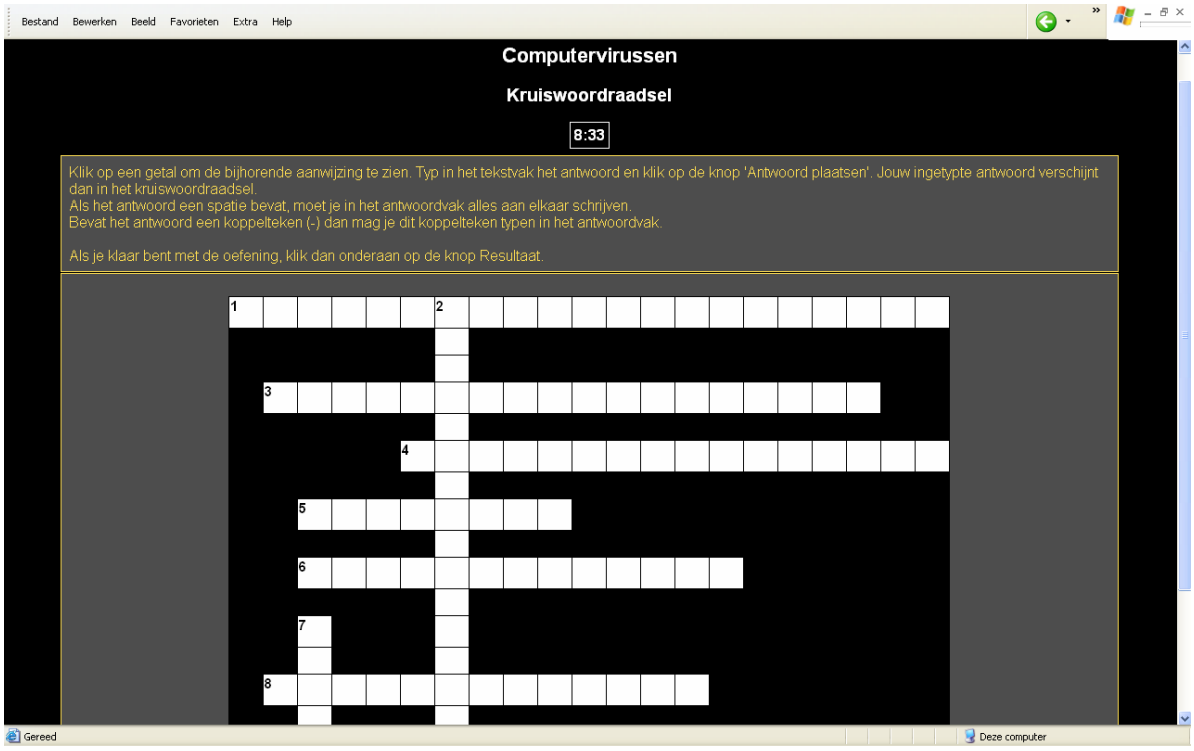
5.1 Home (inleiding)

5.2 Computervirussen

Welke hoofdstukken zijn er terug te vinden bij het deel computervirussen?

- Wat is een computervirus?
- Hoe verspreidt een computervirus zich?
- Soorten computervirussen
- Hulpmiddelen om computervirussen te verbannen
- Werd mijn computer besmet met een computervirus?
- Blijf op de hoogte van de nieuwste computervirussen
- Oefeningen

Kruiswoordraadsel



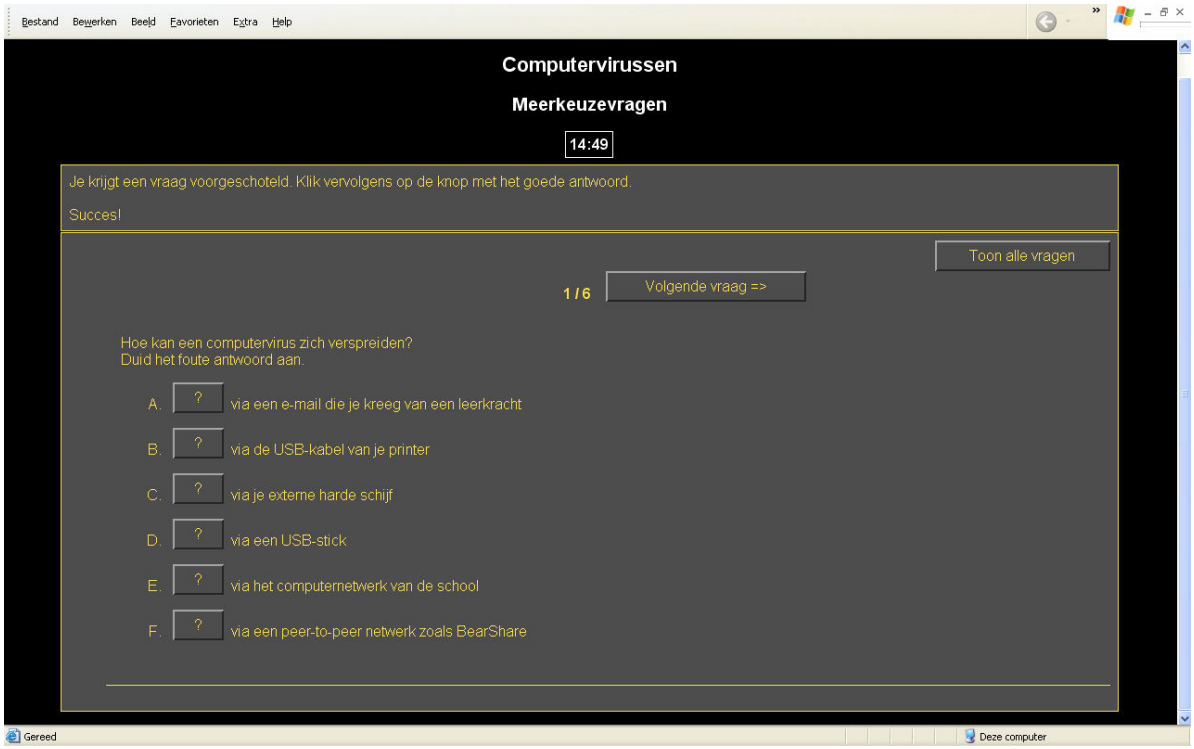
Opgave:
Klik op een getal om de bijhorende aanwijzing te zien. Typ in het tekstvak het antwoord en klik op de knop 'Antwoord plaatsen'. Jouw ingetypte antwoord verschijnt dan in het kruiswoordraadsel.
Als het antwoord een spatie bevat, moet je in het antwoordvak alles aan elkaar schrijven.
Bevat het antwoord een koppelteken (-) dan mag je dit koppelteken typen in het antwoordvak.
Als je klaar bent met de oefening, klik dan onderaan op de knop Resultaat.

Maximum ingestelde tijdsduur:
9 minuten

Oefening:

Nummer	***Vraag***	***Antwoord***
Horizontaal 1	KaZaA, Morpheus, BearShare en LimeWire zijn namen van ... Deze worden meer en meer de ideale virusverdelers want veel mensen maken hiervan gebruik.	peer-to-peer netwerk
Verticaal 2	Een ... scant jouw computer op computervirussen vanop het internet, er wordt dus geen virusscanner gedownload op je computer.	online virusscanner
Horizontaal 3	Wat verwijdert computervirussen en probeert tevens je computer ertegen te beschermen?	antivirusprogramma
Horizontaal 4	Welk soort computervirussen zijn momenteel nog de meest voorkomende computervirussen?	bestandsvirussen
Horizontaal 5	Geef een synoniem voor een hoax.	nepvirus
Horizontaal 6	Hoe noemt men een kwaadaardig computerprogrammaatje dat zich meestal ongemerkt en dus ongevraagd in je computer nestelt?	computervirus
Verticaal 7	Wat verspreidt en vermenigvuldigt zichzelf van computer naar computer terwijl een gewoon computervirus dit doet van bestand tot bestand?	worm
Horizontaal 8	Wat zorgt ervoor dat iemand anders je computer kan 'overnemen' via het internet? Hij/zij kan zelfs strafbare zaken uitvoeren van op jouw computer en dus in jouw naam.	Trojaans paard
Horizontaal 9	Een ... is als een soort mini-antivirusprogramma dat slechts één enkel computervirus herkent en verwijdert.	removal tool

Meerkeuzevragen



Opgave:
Je krijgt een vraag voorgeschoteld. Klik vervolgens op de knop met het goede antwoord. Succes!

Maximum ingestelde tijdsduur:
15 minuten

Oefening:
- Hoe kan een computervirus zich verspreiden? Duid het foute antwoord aan.
    - via een USB-stick
      Feedback: Fout antwoord!
      Een USB-stick is niet schrijfbeveiligd. Een computervirus kan via een USB-stick van de ene naar de andere computer overgebracht worden.
    - via een e-mail die je kreeg van een leerkracht
      Feedback: Fout antwoord!
      Je kunt een e-mail krijgen van een leekracht waarvan de bijlage een computervirus bevat. Waarschijnlijk weet die leerkracht zelfs niet dat hij/zij een computervirus heeft.
    - via de USB-kabel van je printer
      Feedback: Correct antwoord!
      Een computervirus kan zich inderdaad niet verspreiden via de USB-kabel van een printer.
    - via een peer-to-peer netwerk zoals BearShare
      Feedback: Fout antwoord!
      Tegenwoordig worden meer en meer computervirussen verspreid via peer-to-peer netwerken.
    - via je externe harde schijf
      Feedback: Fout antwoord!
      Een externe harde schijf valt ook onder de categorie opslagmedia en kan dus een computervirusdrager zijn.

  - via het computernetwerk van de school
    Feedback: Fout antwoord!
    Als er één computer in een netwerk besmet wordt dan kan het computervirus zich razendsnel verspreiden via het netwerk naar alle andere computers die aangesloten zijn op het netwerk.

- Welk soort computervirussen zijn momenteel het populairst en zorgen dus bij heel veel mensen voor ongenoegen?
  - macrovirussen
    Feedback: Fout antwoord!
  - Trojaanse paarden
    Feedback: Fout antwoord!
  - bestandsvirussen
    Feedback: Correct!
  - spamberichten
    Feedback: Fout antwoord!
    Spamberichten zijn geen computervirussen maar ongewenste e-mails. (zie verder in de website voor meer uitleg)
  - wormen
    Feedback: Fout antwoord!

- Van welke programmeercode maken macrovirussen misbruik?
  - VBA
    Feedback: Fout antwoord!
    VBA staat voor Visual Basic for Applications en wordt vaak gebruikt in het programma Microsoft Access.
  - ingebouwde programmeertaal in Microsoft Office
    Feedback: Correct!
    Van een vriendin krijg je een Word-document doorgestuurd voor het groepswerk Nederlands. Je vult het document wat aan en je wilt de opmaak nog wat wijzigen. Je ziet dat je vriendin een macro gemaakt heeft die een alinea opmaakt met een regelafstand van anderhalf en het lettertype Monotype Corsiva. Let op: deze macro kan misschien wel een macrovirus bevatten.
  - HTML
    Feedback: Fout antwoord!
    De afkorting HTML staat voor Hyper Text Markup Language en met deze programmeertaal kun je webpagina's opmaken.
  - Java
    Feedback: Fout antwoord!
    Java is een objectgeoriënteerde programmeertaal.

- Zijn hoaxes schadelijk voor je computer?
  - ja
    Feedback: Fout antwoord!
    Hoaxes op zich zijn niet schadelijk voor je computer. Let wel op, de inhoud van een hoax mag je niet geloven (hoe erg die soms ook klinkt). Ga niet in op de vraag om het e-mailbericht door te sturen.
  - neen
    Feedback: Correct!
    Hoaxes op zich zijn niet schadelijk voor je computer. Let wel op, de inhoud van een hoax mag je niet geloven (hoe erg die soms ook klinkt). Ga niet in op de vraag om het e-mailbericht door te sturen.

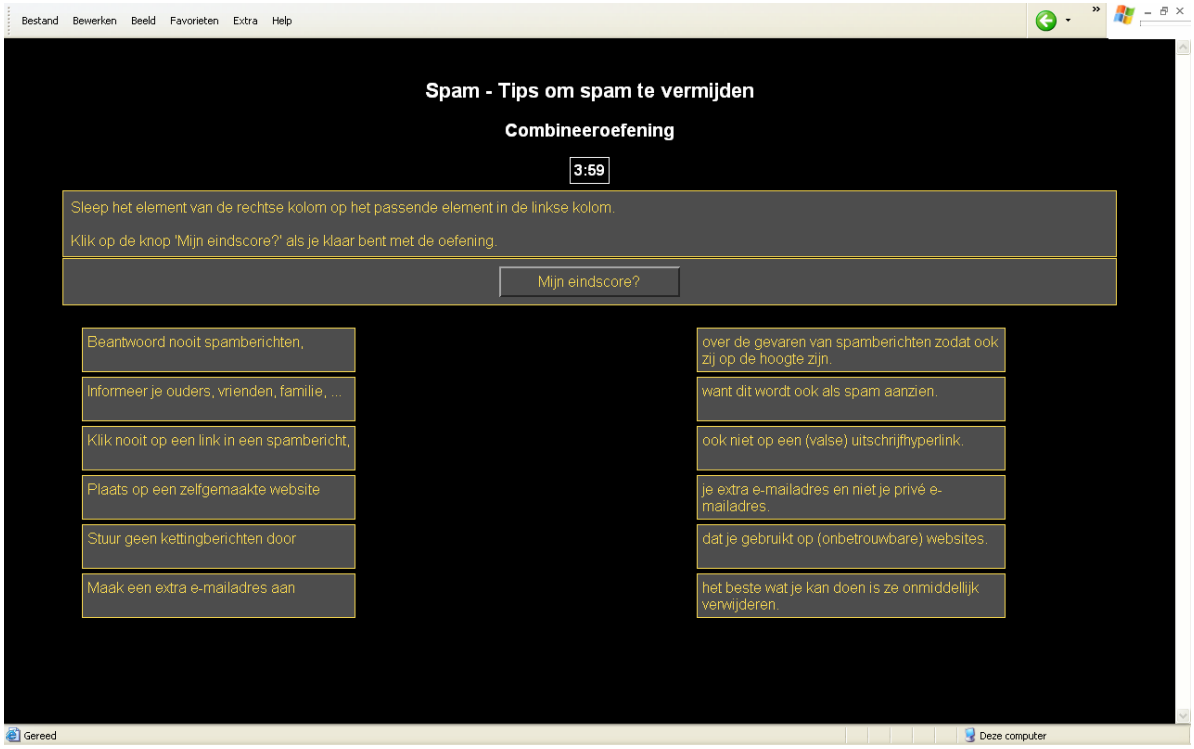
- Je krijgt een e-mail doorgestuurd van een vriend. In die e-mail staat dat je die e-mail naar 10 contactpersonen moet sturen en naar het e-mailadres gratisgsm@hotmail.com. Als je dit doet, krijg je binnen de maand gratis een nieuwe gsm.
  Dit is een ... (duid het correcte aantwoord aan).
  - worm
    Feedback: Fout antwoord!
    Het enige wat een worm doet is, zich verspreiden door zichzelf te kopiëren.
  - hoax
    Feedback: Correct!
    We spreken hier van een hoax of nepvirus. Je mag die mail nog naar 20 mensen sturen, je zal die gsm nooit te zien krijgen. Een vals bericht...
  - Trojaans paard
    Feedback: Fout antwoord!
    Trojaanse paarden dragen een masker: het zien er leuke programmaatjes uit maar ze zijn in feite niet zo leuk. Via een Trojaans paard kan immers iemand anders je computer en/of je identiteit overnemen en in jouw naam criminele computerfeiten plegen.

- Hoe kan een computervirus verwijderd worden?
  Duid het foute antwoord aan.
  - door het internet niet meer te gebruiken
    Feedback: Correct antwoord!
    Het is niet omdat je geen internetverbinding meer heeft dat je computervirus hierdoor verwijderd is, het zal gewoon zijn gangetje blijven gaan. Je zal via het internet wel geen nieuwe computervirussen krijgen, maar let op want je kunt nog op andere manieren dan via het internet computervirussen op je computer krijgen (bijvoorbeeld opslagmedia).
  - door een degelijke online virusscanner
    Feedback: Fout antwoord!
    Een online virusscanner zoals bijvoorbeeld 'Panda Active Scan' kan een computervirus verwijderen.
  - door een removal tool
    Feedback: Fout antwoord!
    Een removal tool kan een computervirus verwijderen.
  - door een degelijk antivirusprogramma
    Feedback: Fout antwoord!
    Een antivirusprogramma kan een computervirus op een efficiënte manier verwijderen.

5.3 Spam

Welke hoofdstukken zijn er terug te vinden bij het deel spam?
- Wat is spam?
- Wat zijn de gevaren van spam?
- Hoe kun je spam proberen te vermijden & hoe ga je ermee om?
- Oefeningen

Combineeroefening



Opgave:
Sleep het element van de rechtse kolom op het passende element in de linkse kolom. Klik op de knop 'Mijn eindscore?' als je klaar bent met de oefening.

Maximum ingestelde tijdsduur:
4 minuten

Oefening:

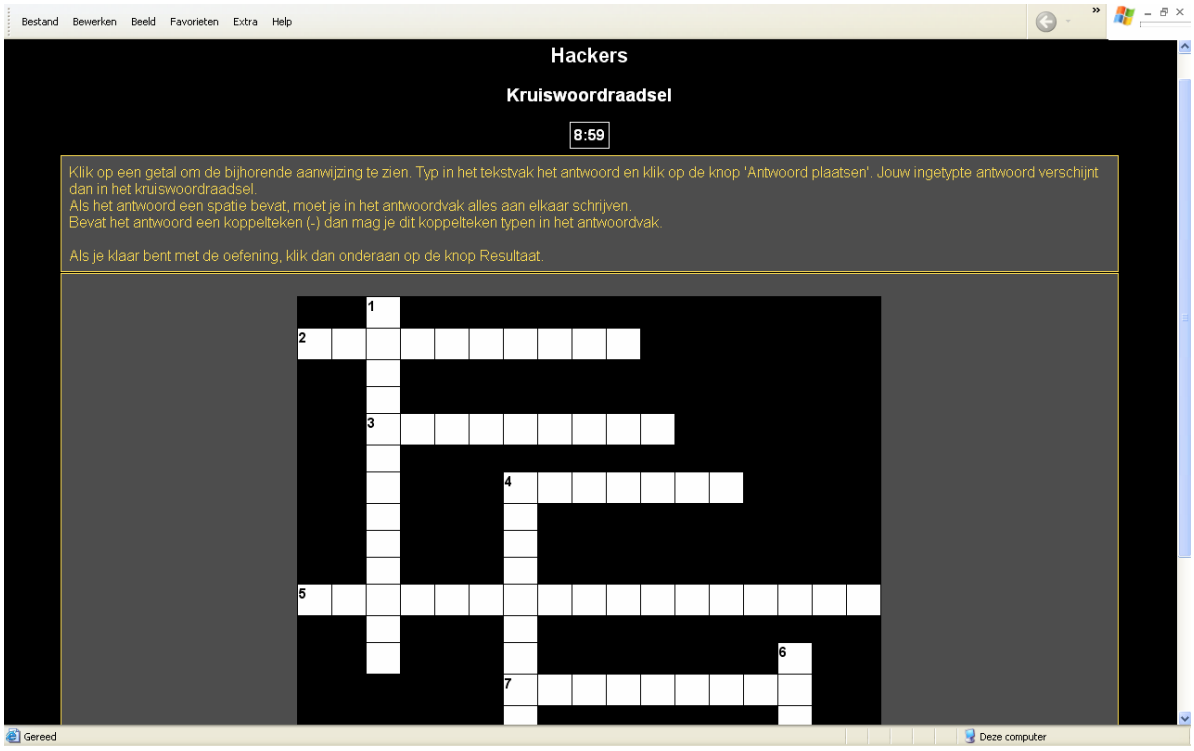
Beantwoord nooit spamberichten	verwijder ze onmiddellijk
Stuur geen kettingberichten door	want dit wordt ook als spam aanzien.
Maak een extra e-mailadres aan	dat je gebruikt op (onbetrouwbare) websites.
Informeer je ouders, vrienden, familie, ...	over de gevaren van spamberichten zodat ook zij op de hoogte zijn.
Klik nooit op een link in een spambericht,	ook niet op een (valse) uitschrijfhyperlink.
Plaats op een zelfgemaakte website	je extra e-mailadres en niet je privé e-mailadres.

5.4 Hackers

Welke hoofdstukken zijn er terug te vinden bij het deel hackers?

- Hackers, crackers en script kiddies
- De verschillende soorten hackers
- Hoe je gegevens beveiligen tegen hackers?
- Oefeningen

Kruiswoordraadsel



Opgave:
Klik op een getal om de bijhorende aanwijzing te zien. Typ in het tekstvak het antwoord en klik op de knop 'Antwoord plaatsen'. Jouw ingetypte antwoord verschijnt dan in het kruiswoordraadsel.
Als het antwoord een spatie bevat, moet je in het antwoordvak alles aan elkaar schrijven.
Bevat het antwoord een koppelteken (-) dan mag je dit koppelteken typen in het antwoordvak.
Als je klaar bent met de oefening, klik dan onderaan op de knop Resultaat.

Maximum ingestelde tijdsduur:
9 minuten

Oefening:

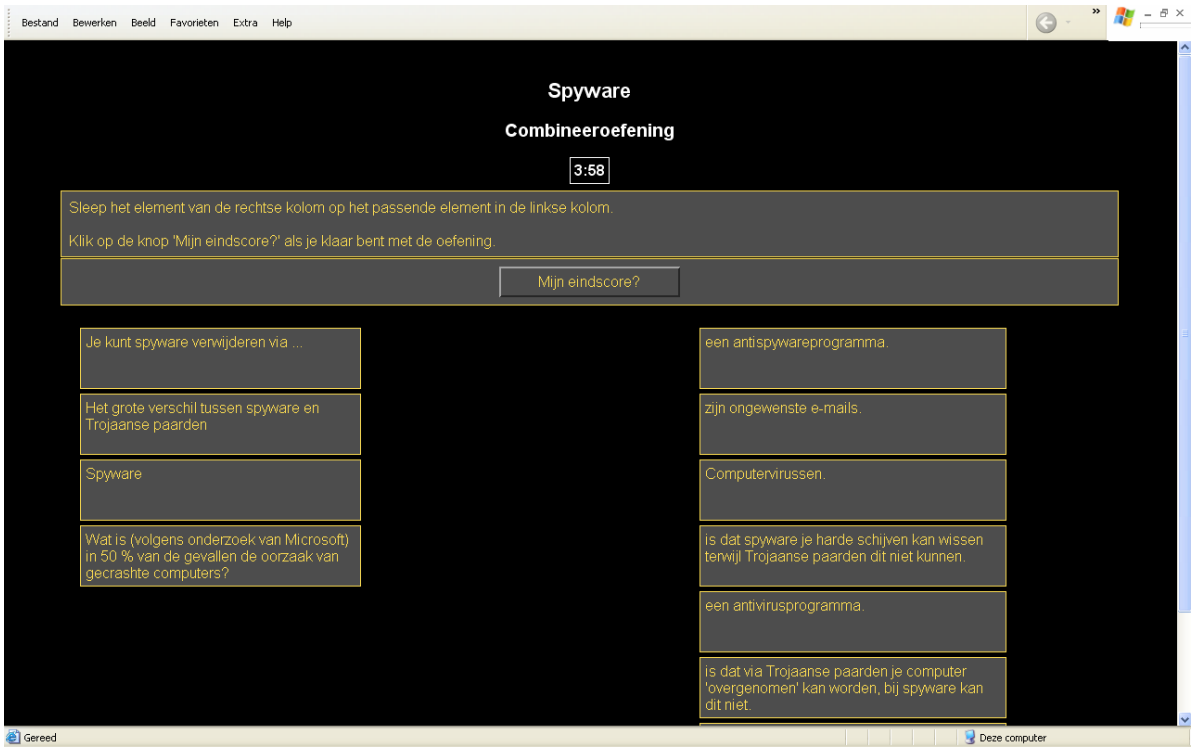
Nummer	***Vraag***	***Antwoord***
Verticaal 1	Welk soort computerinbrekers zijn het meest bedreigend voor de gewone computergebruiker en zijn nog aan het leren om in computers in te breken?	script kiddies
Horizontaal 2	Met wat kun je je e-mailaccount, gebruikersaccount, ... beveiligen zodat hackers er minder vlug toegang toe krijgen?	wachtwoord
Horizontaal 3	Gratis firewall's hebben meestal enkel de mogelijkheid om inkomende ... te controleren en niet de uitgaande.	pakketjes
Horizontaal 4	Hoe noem je het soort mensen die zonder kwade bedoelingen inbreken in een computersysteem om vervolgens de veiligheidslekken te melden aan de	hackers

	maker(s) van het programma.	
Verticaal 4	Hoe noemen we de mensen die sommige bedrijven inhuren om in te breken in hun eigen computersysteem en/of in dat van de concurrent?	huurhackers
Horizontaal 5	Waar maakt een hacker in veel gevallen gebruik van om een computersysteem te hacken?	veiligheidslekken
Verticaal 6	Welk soort computerinbrekers hebben de bedoeling om dingen stuk te maken en zo te laten zien wat hij/zij kan? Hij/zij wil trouwens ook geld slaan uit zijn computerinbraak.	crackers
Horizontaal 7	Een ... kan alle toetsaanslagen opslaan waardoor een hacker je wachtwoord uit al deze toetsaanslagen kan filteren. In de meeste gevallen weet je niet dat het programmaatje op je computer staat.	keylogger
Horizontaal 8	Hoe noemen we de softwarebescherming tegen hackersaanvallen?	firewall
Horizontaal 9	Via een firewall kun je bepaalde ... (bijvoorbeeld ... 80 en 25 voor internet en e-mail) toestemming geven om te communiceren met het internet terwijl je anderen kunt blokkeren.	poorten

5.5 Spyware

Welke hoofdstukken zijn er terug te vinden bij het deel spyware?
- Wat is spyware?
- Wat zijn de nadelen van spyware?
- Hoe kun je spyware voorkomen?
- Hoe kun je spyware verwijderen?
- Oefeningen

Combineeroefening



Opgave:
Sleep het element van de rechtse kolom op het passende element in de linkse kolom. Klik op de knop 'Mijn eindscore?' als je klaar bent met de oefening.

Maximum ingestelde tijdsduur:
4 minuten

Oefening:

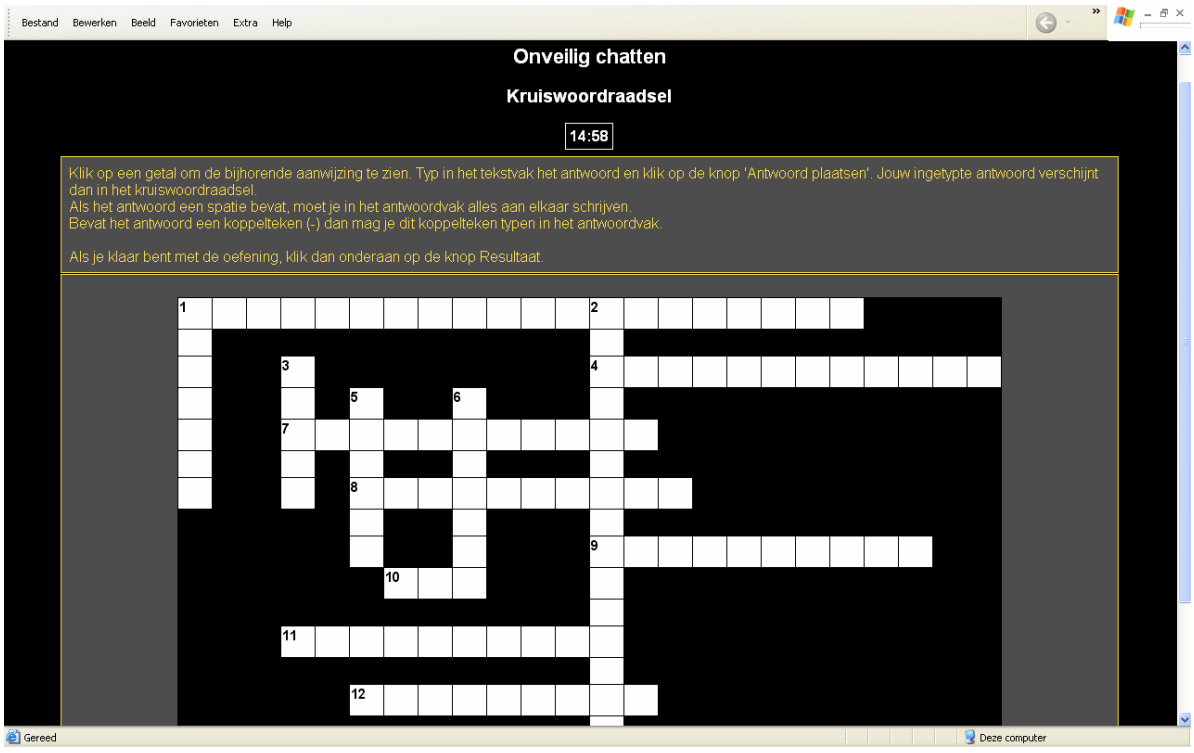
Spyware	is software (een programma).
Het grote verschil tussen spyware en Trojaanse paarden	is dat via Trojaanse paarden je computer 'overgenomen' kan worden, bij spyware kan dit niet.
Wat is (volgens onderzoek van Microsoft) in 50 % van de gevallen de oorzaak van gecrashte computers?	Spyware.
Je kunt spyware verwijderen via ...	een antispywareprogramma.
	is dat spyware je harde schijven kan wissen terwijl Trojaanse paarden dit niet kunnen.
	zijn ongewenste e-mails.
	een antivirusprogramma.
	Computervirussen.

5.6 Onveilig chatten

Welke hoofdstukken zijn er terug te vinden bij het deel onveilig chatten?

- Statistieken
- Wat kan er fout lopen in cyberspace?
- Chatboxen
- Wat als het uit de hand loopt?
- 'Veilig' chatten
- Belangrijke chattips
- Oefeningen

Kruiswoordraadsel



Opgave:

Klik op een getal om de bijhorende aanwijzing te zien. Typ in het tekstvak het antwoord en klik op de knop 'Antwoord plaatsen'. Jouw ingetypte antwoord verschijnt dan in het kruiswoordraadsel.
Als het antwoord een spatie bevat, moet je in het antwoordvak alles aan elkaar schrijven.
Bevat het antwoord een koppelteken (-) dan mag je dit koppelteken typen in het antwoordvak.
Als je klaar bent met de oefening, klik dan onderaan op de knop Resultaat.

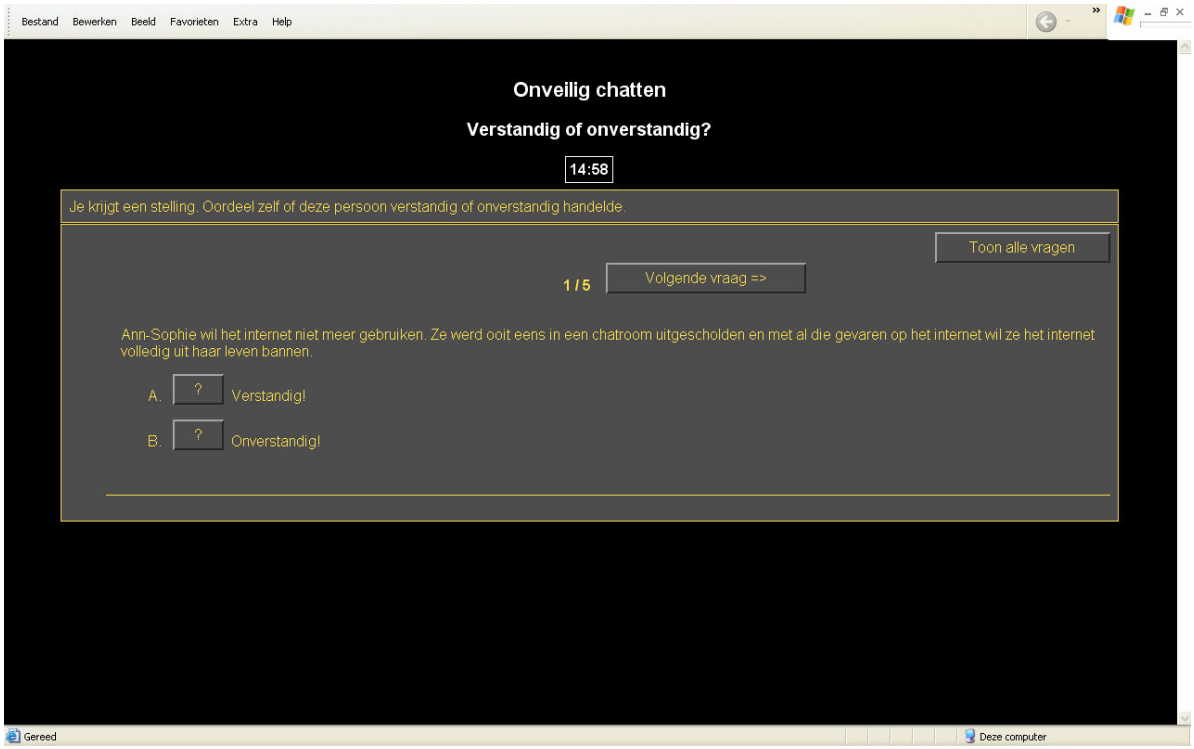
Maximum ingestelde tijdsduur:
15 minuten

Oefening:

Nummer	***Vraag***	***Antwoord***
Horizontaal 1	Let op met de ... die je geeft aan een chatvriend die je nog niet zo goed kent. Zeg tegen hem/haar dat je die informatie nog niet met hem wilt delen of zeg een leugentje voor je eigen bestwil.	persoonlijke gegevens
Verticaal 1	Om in een beveiligde chatroom te kunnen chatten, moet je je eID gebruiken en je eID-... invoeren.	pincode
Verticaal 2	Chatboxen die je moet downloaden en waarbij je zelf bepaalt wie je al dan niet 'accepteert' in je chatlijst.	gesloten chatboxen
Verticaal 3	Dit is het Belgisch overheidsmeldpunt voor internetmisbruik. Hier kun je klacht neerleggen voor om het even welke informaticacriminaliteit. Deze mensen zorgen er dan voor dat je klacht bij de juiste instantie terecht komt.	ecops
Horizontaal 4	Als iemand echt te ver is gegaan via het chatten en je je bedreigd voelt dan kun je een klacht indienen. Zorg ervoor dat je dan alle gegevens van die chatter verzamelt, maak ook een ... van alle onleuke zaken die hij/zij gedaan heeft.	schermafdruk
Verticaal 5	Let op met wat je doet voor de ... want denk eraan dat de persoon waarmee je een gesprek voert die beelden kan opslaan en eventueel verspreiden. Je bepaalt nog altijd zelf wat je doet dus laat je niet chanteren en of verplicht voelen om bepaalde zaken te doen.	webcam
Verticaal 6	Babbelen (typen) met iemand via het internet.	chatten
Horizontaal 7	Welk soort chatbox is de chatbox van TMF?	open chatbox
Horizontaal 8	Een persoon waarmee je regelmatig chat.	chatvriend
Horizontaal 9	Elke chatbox heeft zijn eigen ... Het is aan te raden die te lezen alvorens je chat; ze bevatten je rechten en plichten.	chatregels
Horizontaal 10	De populairste gesloten chatbox en tevens een product van Microsoft.	MSN
Horizontaal 11	Mensen kunnen zich op het internet anders voordoen dan ze in werkelijkheid zijn. Ze kunnen een andere ... aannemen.	identiteit

Horizontaal 12	Een ervaren chat-kenner die alle gebeurtenissen in de chatroom volgt en erop toekijkt dat iedereen zich aan de regels van de chatbox houdt.	moderator
Horizontaal 13	Vele chatters liegen over hun ... (tip: ik ben 16 jaar).	leeftijd

Meerkeuzevragen



Opgave:
Je krijgt een stelling. Oordeel zelf of deze persoon verstandig of onverstandig handelde.

Maximum ingestelde tijdsduur:
15 minuten

Oefening:

- Lisa leerde 5 maanden geleden Mathieu kennen op de chatbox van TMF. Sindsdien heeft ze al veel met hem gechat en hem heel wat zaken toevertrouwd over haar beste vriendin Eva. Vandaag vraagt Mathieu aan Lisa of hij het e-mailadres van Eva mag hebben zodat hij ook met haar kan kennismaken. Hij zegt dat hij dan beter de vriendschapsrelatie tussen Eva en Lisa zal begrijpen. Lisa ziet hier geen problemen in en geeft hem het e-mailadres van Eva.
    - Verstandig!
      Feedback: Fout antwoord!
      Geef nooit persoonlijke gegevens van je vrienden door aan andere personen. Misschien wil Eva wel geen contact met Mathieu. Het zou dan erg vervelend voor Eva zijn dat Mathieu haar e-mailadres heeft.
    - Onverstandig!
      Feedback: Correct antwoord!

Let op met de persoonlijke gegevens die je blootgeeft over jezelf maar geef zeker geen persoonlijke gegevens van een vriend of vriendin door. Je weet nooit dat Mathieu slechte bedoelingen heeft. Als je toch Eva's e-mailadres aan Mathieu wilt geven, vraag dit dan eerst aan Eva of je dit mag doen.

- Msn gebruik ik enkel en alleen voor goede vrienden die ik ken van op school, jeugdbeweging, ... Als ik een persoon leuk vind op een open chatbox dan spreken we op die chatbox nog enkele keren af. Als ik hem dan nog steeds leuk vind, voeg ik hem toe op mijn tweede e-mailadres dat ik enkel en alleen gebruik voor chatvrienden die ik leerde kennen op een open chatbox.
    - Verstandig!
      Feedback: Correct antwoord!
      Jij weet hoe je veilig moet chatten!
    - Onverstandig!
      Feedback: Fout antwoord!
      Je zou beter wel een tweede e-amiladres hebben voor mensen die je leerde kennen via een open chatbox. Word je plots door zo'n 'chatbuddy' overspoeld met onleuke mails, dan kun je nog steeds beslissen om dat e-mailadres niet meer te gebruiken.

- Sander is 18 jaar en is dol op auto's. Op een dag chat hij op een open chatbox met Chiel. Chiel is 20 jaar en heeft zonet van zijn ouders een Porsche cadeau gekregen. Toevallig zijn Porsches de lievelingsauto's van Chiel. Chiel nodigt Sander uit om een ritje te maken, ze kunnen eens samen naar de zee rijden. Chiel komt Sander ophalen om 15.00 uur bij hem thuis.
    - Verstandig!
      Feedback: Fout antwoord!
      Geloof niet alles wat er in de chatroom wordt verteld. Heeft Chiel wel een Porsche? Heet de chatvriend van Sander wel Chiel? Is Chiel echt nog maar 20 jaar? ...
    - Onverstandig!
      Feedback: Correct antwoord!
      Het is goed dat je niet alles gelooft wat er in de chatroom wordt verteld. Heeft Chiel wel een Porsche? Heet de chatvriend van Sander wel Chiel? Is Chiel echt nog maar 20 jaar? ...

- Stéphanie en Joerik zijn een koppeltje. De laatste tijd gaat het niet zo goed tussen hen, er zijn wat kleine strubbelingen. Op een dag krijgt Stéphanie een e-mail van Joerik. In die e-mail scheldt Joerik haar de huid vol en breekt hij met haar. Stéphanie zit diep in de put en weet zich geen raad. Ze sluit zich van de buitenwereld af en wil met niemand contact. Ze is geschokt over de e-mail. Ook met Joerik heeft Stéphanie nog geen contact opgenomen, ze is ontzettend boos op hem.
    - Verstandig!
      Feedback: Fout antwoord!
      Dit verhaal kan inderdaad kloppen. Toch moet Stéphanie eerst en vooral eens controleren of Joerik haar die e-mail heeft gestuurd. Het zou kunnen zijn dat iemand het paswoord van de e-mailbox van Joerik had en op die manier in de naam van Joerik een e-mail stuurde naar Stéphanie.
    - Onverstandig!
      Feedback: Correct antwoord!
      Stéphanie zou best eerst eens vragen aan Joerik of hij haar echt wel die e-mail heeft gestuurd. Het zou kunnen zijn dat iemand het paswoord van de e-mailbox van Joerik had en op die manier in de naam van Joerik een e-mail stuurde naar Stéphanie.

- Ann-Sophie wil het internet niet meer gebruiken. Ze werd ooit eens in een chatroom uitgescholden en met al die gevaren op het internet wil ze het internet volledig uit haar leven bannen.
    - Verstandig!
      Feedback: Fout antwoord!
      Het is natuurlijk Ann-Sophie's eigen mening maar het is niet verstandig... Ann-Sophie ziet de vele positieve kanten niet van het internet zoals vb. informatie opzoeken, communiceren met je 'echte' vrienden, tickets reserveren, ... Toen Ann-Sophie werd uitgescholden op die chatroom, moest ze contact opgenomen hebben met de moderator van de chatbox of erover gesproken hebben met vertrouwenspersonen.
    - Onverstandig!
      Feedback: Correct antwoord!
      Het is natuurlijk Ann-Sophie's eigen mening maar het is niet verstandig... Ann-Sophie ziet de vele positieve kanten niet van het internet zoals vb. informatie opzoeken, communiceren met je 'echte' vrienden, tickets reserveren, ... Toen Ann-Sophie werd uitgescholden op die chatroom, moest ze contact opgenomen hebben met de moderator van de chatbox of erover gesproken hebben met vertrouwenspersonen.

5.7 Cyberpesten

Welke hoofdstukken zijn er terug te vinden bij het deel cyberpesten?

- Wat is cyberpesten?
- Acties tegen cyberpesten
- Waar gebeurd

Besluit

Door dit eindwerk heb ik nog een beter beeld gekregen van de gevaren die schuilen op het internet. Het was voor mij beslist een zeer leerrijke ervaring.

In het kader van dit eindwerk heb ik vorig jaar het eerste Veilig Internet Congres bijgewoond te Amsterdam. Dit congres wordt jaarlijks georganiseerd door De Kinderconsument en is een aanrader voor elke leerkracht, die zich wat meer in deze materie wil verdiepen.

Het internet bevat meer en meer gevaren en het is belangrijk dat ook de jongeren hierover geïnformeerd worden. Kinderen en jongeren moeten beschermd worden, en dit is niet anders op het internet. Het is daarom heel belangrijk dat zowel ouders als leerkrachten hieraan meewerken en zo de wereld wat veiliger helpen maken.

Bijlagen

Bijlage 1: brochure 'Hoe digibewust bent u?' (van pagina 147 tot en met pagina 163).

Bijlage 2: jongerengids 'Als een visje door het net' (van pagina 164 tot en met pagina 187).

Bijlage 1: brochure 'Hoe digibewust bent u?'

HOE DIGIBEWUST BENT U?

TIPS VOOR IN DE ONLINE WERELD

DIGI bewust

DIGIBEWUST

BENT U ?

BENT U DIGIBEWUST?

Internet en e-mail zijn niet meer weg te denken uit ons dagelijkse leven. Thuis, op school of op het werk: bijna iedereen maakt er wel gebruik van. En de mogelijkheden groeien alleen maar. We kunnen eenvoudig op internet zoeken naar tekst, beeld en geluid. We chatten en gamen online. We vinden oude vrienden en klasgenoten terug op internet. We downloaden muziek en films. We kunnen van alles via internet kopen én verkopen. En wat dacht u van het online regelen van uw bankzaken?

Digibewust zijn betekent dat u gebruikmaakt van de mogelijkheden van internet. En dat terwijl u zich bewust bent van de eventuele gevaren en risico's die aan dit gebruik kleven en daar ook maatregelen tegen neemt. Want helaas hebben de mogelijkheden en voordelen van internet ook een schaduwzijde. Denk bijvoorbeeld aan virussen en spam.

Deze brochure helpt u digibewust te zijn. U krijgt uitleg over de toepassingen van internet en u leest wat de mogelijke gevaren en risico's zijn van bijvoorbeeld surfen, e-mailen en chatten. En u krijgt vooral ook tips over wat u kunt doen om uw computer en uzelf te beschermen. Daarnaast leest u hoe u uw kind veilig het internet kunt laten op gaan. Deze tips herkent u aan het icoontje*. Met een aantal eenvoudige maatregelen kunt u op een bewuste en veilige manier profiteren van de mogelijkheden van internet!

Wilt u na het lezen van deze brochure meer weten?

Kijk dan op www.digibewust.nl!

*

INHOUDS-OPGAVE

Test uw kennis! Hoe digibewust bent u?

Test uw kennis over de online wereld en vindt uit hoe digibewust u bent. Kruis aan welk antwoorden het best bij u passen, tel uw punten op en bekijk uw score!

1. Wat doet u allemaal digitaal?
a. Ik heb een aantal klokken in huis die digitaal de tijd aangeven.
b. Ik e-mail en ik surf.
c. Ik e-mail, surf, chat en bankier online.
d. Ik e-mail, surf, chat, game, bankier online, zit regelmatig op een veilingsite en koop regelmatig wat online.

2. Hoe beveiligt u uw computer?
a. Beveiligen? Ik trek de stekker eruit als ik voor een langere periode niet thuis ben.
b. Een firewall moet genoeg zijn.
c. Met een firewall, een virusscanner en antispywaresoftware die ik regelmatig update. En ik heb ook een pop-up blocker geïnstalleerd en ik maak regelmatig back-ups.
d. Met een firewall en een virusscanner.

3. Wat voor wachtwoord heeft u?
a. Is dit een strikvraag? Dat ga ik jou natuurlijk niet vertellen!
b. O, eentje die heel makkelijk te onthouden is: mijn initialen en geboortedatum.
c. Een heel ingewikkelde, zo ingewikkeld dat ik hem maar op een geel briefje aan mijn beeldscherm heb gehangen.
d. Ik heb meer dan één wachtwoord. Ik vertel deze nooit aan iemand en ik zorg altijd dat een wachtwoord uit minimaal 8 karakters bestaat, waarvan minimaal 1 cijfer en een leesteken, bijvoorbeeld VlaFlip!59.

4. Wat is een profielsite?
a. Dat is toch iets voor de jeugd? Daar hou ik mij niet mee bezig.
b. Geen idee.
c. Een site waar mensen foto's en informatie over zichzelf kunnen plaatsen en vrienden kunnen toevoegen.
d. Een site waar iemand iets over zichzelf vertelt.

5. Wat doet u met e-mail van onbekende afzenders?
a. Die open ik. Ik ben veel te nieuwsgierig wie mij mailt.
b. Die gooi ik gelijk ongelezen in de prullenbak.
c. Ligt aan het onderwerp van de mail, de eigenschappen en hoe mijn spamfilter hem heeft geclassificeerd.
d. Openen en lezen natuurlijk. En als het een leuke mail is stuur ik hem door naar familie en vrienden.

6. Weet u wat uw kinderen op internet doen?
a. Nee. Dat hoef ik ook niet te weten. Ik vertrouw mijn kinderen.
b. Ja, mijn computer volzetten met spyware, illegale downloadprogramma's en andere troep.
c. Ja, ik praat met mijn kinderen over wat zij op internet doen en vraag hen regelmatig mij dit ook te laten zien.
d. Ja, ik praat met hen over wat zij op internet doen, ik geef voorlichting en stel regels.

7. Vult u uw gegevens wel eens op internet in?
a. Heel vaak, je weet maar nooit wat je kan winnen!
b. Ja, maar met mijn bankgegevens ben ik voorzichtig.
c. Ik kijk altijd eerst door wie en waarom mijn informatie wordt gevraagd en wat ze met mijn gegevens gaan doen. Als ik het niet vertrouw dan vul ik niets in.
d. Nee, ik laat nooit gegevens achter op internet.

8. Downloaden en delen: wat mag wel?
a. Een thuiskopie maken van een film als die uitsluitend voor mezelf bestemd is.
b. Een film of muziek downloaden en die weer via mijn file-sharing netwerk aan anderen aanbieden.
c. Alle nieuwste games downloaden en onder mijn vrienden verspreiden.
d. Mijn eigen fantastische zelfgemaakte films, foto's en muziek delen.

9. Waar let u op bij het doen van uw online bankzaken?
a. Op het slotje onder aan de pagina, waarop ik even op klik om het SSL-certificaat te bekijken en op de code https:// voor de URL die aangeeft dat ik mij op een beveiligde site bevind en op de URL zelf.
b. Moet ik ergens op letten?
c. Ja natuurlijk, ik let op of mijn rekening nog courant is.
d. Ik doe niet aan online bankieren. Ik vertrouw dat niet.

10. Als iemand u tijdens het spelen van een online game aanspreekt met "OMG u n00b, WTF?!", dan bedoelt hij:
a. Hoi! Hoe gaat het met jou?
b. Wat doe jij nu in hemelsnaam, domme nieuwkomer?!
c. Goed gespeeld!
d. Hoi! Want to fight?

SCORETABEL

1. a. 0 b. 2 c. 3 d. 5
2. a. 0 b. 2 c. 5 d. 3
3. a. 3 b. 0 c. 2 d. 5
4. a. 2 b. 0 c. 5 d. 3
5. a. 0 b. 2 c. 5 d. 0
6. a. 2 b. 0 c. 3 d. 5
7. a. 0 b. 3 c. 5 d. 2
8. a. 5 b. 0 c. 0 d. 2
9. a. 5 b. 0 c. 0 d. 0
10. a. 0 b. 5 c. 2 d. 0

UW SCORE

0-15 punten
U bent duidelijk niet bekend met de online wereld, laat staan het veilig gebruik ervan. En dat terwijl het u zoveel mogelijkheden en voordelen kan bieden. Lees dit boekje: er gaat een wereld voor u open. U weet straks niet alleen wat er allemaal te halen valt, maar ook hoe u goed voorbereid de online wereld kunt betreden.

15-35 punten
U heeft de online wereld waarschijnlijk pas net ontdekt en bent nu zoekende naar de beste en veiligste manier om de mogelijkheden ervan te benutten. Dit boekje helpt u daarbij. Gebruik de tips en heeft u meer informatie nodig, kijk dan ook eens op **www.digibewust.nl.** Wordt digibewust!

35-50 punten
U bent goed bezig! Lees dit boekje vooral nog even door, want er staan vast nog wel wat tips in die u kunt gebruiken. Of wellicht kunt u met dit boekje in de hand mensen in uw omgeving helpen bewust veilig de online wereld in te gaan!

Uw computer

Een van de eerste stappen om veilig de online wereld te betreden, is het beveiligen van uw computer. Want dat is niet alleen uw deur tot deze online wereld, maar het is ook de deur naar úw wereld. U bewaart namelijk (bewust of onbewust) allerlei persoonlijke informatie, documenten, bestanden, foto's, films en/of muziek op uw computer. En u wilt niet dat deze gestolen worden of beschadigd raken. Daarom is het noodzakelijk uw computer te beveiligen tegen virussen, hacking en andere gevaren van buiten af.

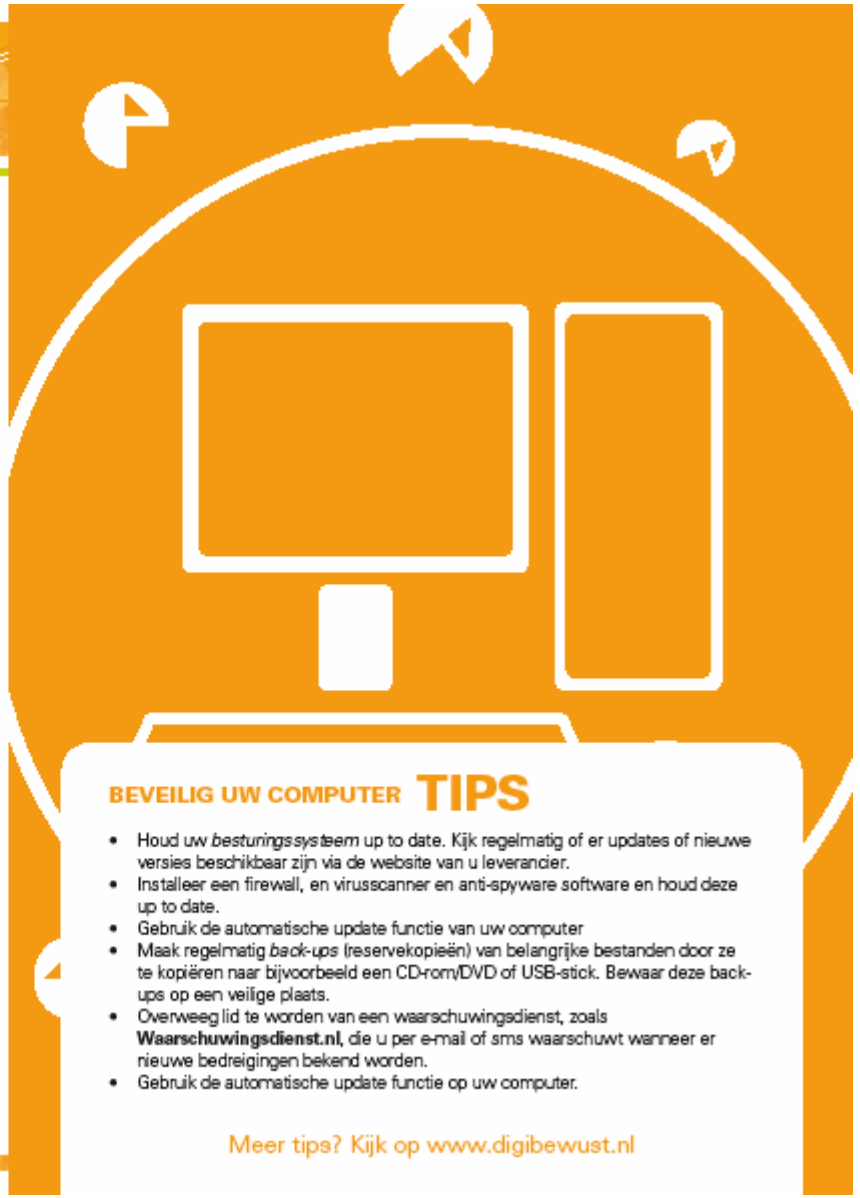
WAT U MOET WETEN

Een **virus** is een softwareprogrammaatje dat probeert misbruik te maken van uw computer. Virussen kunnen zonder dat u het weet de instellingen van uw computer beschadigen of veranderen zodat uw computer gebruikt kan worden voor het verspreiden van bijvoorbeeld porno of **spam** (zie p. 10). Uw computer is dan onderdeel van een zogenaamd **zombienetwerk** of **botnet**, een netwerk van een groot aantal computers die allemaal besmet zijn met eenzelfde bot. Een bot is een programma dat meestal via een virus op uw computer terecht komt en vervolgens vanuit één centraal punt opdrachten krijgt, bijvoorbeeld om spam te versturen.

Bij computercriminaliteit spreken we over **hackers**. Maar dat is niet helemaal juist. De correcte betekenis van hacker komt namelijk meer in de buurt van computerexpert! Beter is te spreken over **crackers** of computercriminelen. Zij breken in op een computer of een netwerk, of leggen websites lam. De gevolgen van computercriminaliteit kunnen variëren van misbruik van uw persoonlijke gegevens (bankrekeninginformatie, creditcardnummer, enz.) en het beschadigen van data tot het gebruiken van uw computer om ongewenste handelingen te verrichten (het opslaan van illegaal materiaal bijvoorbeeld).

Spyware is software die stiekem op uw computer geplaatst wordt en daarna, zonder dat u het in de gaten heeft, gegevens doorstuurt (naar bijvoorbeeld adverteerders). Dit kunnen gegevens zijn over uw online koopgedrag of de websites die u bezoekt. Maar er bestaat ook spyware die op zoek gaat naar uw bank- en creditcardgegevens.

Adware is software die u gratis gebruik laat maken van een programma of dienst. In ruil hiervoor worden er (vaak ongemerkt) gegevens over uw surfgedrag doorgegeven en krijgt u grote hoeveelheden advertenties te zien, al dan niet in pop-ups.



BEVEILIG UW COMPUTER TIPS

- Houd uw *besturingssysteem* up to date. Kijk regelmatig of er updates of nieuwe versies beschikbaar zijn via de website van u leverancier.
- Installeer een firewall, en virusscanner en anti-spyware software en houd deze up to date.
- Gebruik de automatische update functie van uw computer
- Maak regelmatig *back-ups* (reservekopieën) van belangrijke bestanden door ze te kopiëren naar bijvoorbeeld een CD-rom/DVD of USB-stick. Bewaar deze back-ups op een veilige plaats.
- Overweeg lid te worden van een waarschuwingsdienst, zoals **Waarschuwingsdienst.nl**, die u per e-mail of sms waarschuwt wanneer er nieuwe bedreigingen bekend worden.
- Gebruik de automatische update functie op uw computer.

Meer tips? Kijk op www.digibewust.nl

Chatten

Chatten is 'kletsen' door het versturen van korte tekstberichten via internet. Chatten geeft u de mogelijkheid online met andere mensen in contact te komen en gesprekken aan te gaan. Op deze manier kunt u ook online uw sociale contacten onderhouden en uw sociale netwerk uitbreiden. Vooral onder jongeren is chatten erg populair: 90% van de jongeren chat!
Door een aantal zaken goed in de gaten te houden voorkomt u dat u (of uw kind) via het chatten met kwaadwillende personen in contact komt of berichten met ongewenste inhoud ontvangt.

WAT U MOET WETEN

Een **chatroom (of chatbox)** is een virtuele ruimte op internet waar mensen met elkaar kunnen chatten. *Openbare chatrooms* zijn onderdeel van een website en zijn toegankelijk voor iedereen. Bekende openbare chatrooms zijn *tmf.nl* en *chatten.nl*. Onder kinderen is op dit moment *Habbohotel* populair. Maar er zijn ook diverse chatrooms voor specifieke doelgroepen of over speciale onderwerpen. In sommige openbare chatrooms zijn *moderators* aanwezig. Zij volgen de gesprekken en kunnen beslissen om bepaalde boodschappen niet te laten verschijnen of mensen uit de chatroom te zetten. In *besloten chatrooms* (waarvoor u software moet downloaden) moet u toestemming krijgen om met andere te chatten of toestemming geven aan iemand om met u te chatten.

Een **Instant Messenger** (IM) is een softwareprogramma waarmee u kunt chatten. U chat (veelal één op één) vervolgens met personen die u heeft toegevoegd aan uw contactlijst. U kunt in een oogopslag zien wie van uw contacten is ingelogd en er vervolgens mee chatten. De bekendste Instant Messenger is *MSN*.

Op een **profielsite** kunt u uw persoonlijke pagina of profiel aanmaken. Zo'n profiel bestaat bijvoorbeeld uit een stukje tekst met foto's over uzelf. Profielsites zijn meestal openbaar: iedereen kan uw profiel bekijken. Sommige profielsites hebben ook netwerkmogelijkheden waarbij u uw profiel kunt koppelen aan dat van vrienden. Ook kunnen digitale dagboeken (weblogs) worden bijgehouden. Populaire en bekende profielsites zijn *Hyves*, *CU2* en *Sugababes/Superdudes*.

Een **webcam** is een kleine videocamera waarmee u via internet beelden kunt verzenden. Zo kunt u bijvoorbeeld tijdens het MSN'en beelden ontvangen van uw gesprekspartner. Dit wordt cammen genoemd.

VEILIG CHATTEN TIPS

- Wees voorzichtig met het vermelden van persoonlijke gegevens als achternaam, adres of (mobiele) telefoonnummer.
- Wees voorzichtig bij het cammen met personen die u niet kent. Hij/zij kan de webcambeelden opslaan en hergebruiken.
- Spreek bij ontmoetingen met iemand die u niet kent af in een openbare gelegenheid (café, bibliotheek) en neem iemand mee.
- Bedenk dat mensen op internet makkelijk een andere identiteit kunnen aannemen.
- Controleer of er moderators in de openbare chatroom aanwezig zijn, of er een mogelijkheid is om andere chatters te blokkeren en of er een helpfunctie is (zie ook **www.chatinfo.nl**).

HELP UW KIND TIPS

- Bereid uw kind voor op wat hij/zij kan tegenkomen in de chatroom: ongewenste berichten, grof taalgebruik, *digitaal pesten*, enzovoort.
- Blijf betrokken bij wat uw kind op internet doet. Neem zelf ook een kijkje in een chatroom en praat met uw kind over internet.
- Zet de computer bij voorkeur in het zicht, bijvoorbeeld in de huiskamer.
- Weet waar uw kind chat en met wie.
- Spreek tijden af wanneer en hoe lang uw kind mag chatten.

Meer tips? Kijk op www.digibewust.nl

E-mailen

Het gebruik van e-mail is inmiddels redelijk ingeburgerd. Veel mensen, van jong tot oud, beschikken over één of meerdere e-mailadressen waarmee ze berichten kunnen versturen over het internet. Met een e-mail kunt u ook allerlei bestanden (beeld, video, geluid, software) versturen als zogenaamd *attachment* (bijlage). E-mailen is een snelle, gemakkelijke en veelgebruikte manier van communiceren. Om veilig te e-mailen is het van belang te weten wat de risico's zijn en hoe u problemen kunt voorkomen.

WAAR U OP MOET LETTEN

Spam is e-mail die zogenaamde spammers in grote hoeveelheden en ongevraagd versturen en die vervolgens in uw mailbox kan belanden. De inhoud van een spambericht loopt uiteen van reclame tot oplichtingspogingen. Op www.digibewust.nl staat hoe u spam kunt tegengaan.

Een **virus** is een softwareprogrammaatje dat probeert misbruik te maken van uw computer. Virussen kunnen zonder dat u het weet de instellingen van uw computer beschadigen of veranderen zodat uw computer gebruikt kan worden voor het verspreiden van bijvoorbeeld porno of spam. Een virus kan via e-mail worden verspreid. Op www.digibewust.nl leest u hoe u virussen kunt tegengaan.

Phishing is een vorm van oplichting via het internet. Door een nepsite of e-mail probeert de oplichter uw persoonlijke gegevens als creditcardnummer, pincode, sofinummer etc. te achterhalen. Deze e-mail of website lijkt te zijn van een betrouwbare instantie zoals uw creditcardmaatschappij of bank. Uw bank zal echter nooit via de e-mail naar dit soort gegevens vragen. Op www.digibewust.nl leest u hoe u phishing e-mails en websites kunt herkennen.

Een **hoax** is een onzin-mail. Soms worden er in deze mail grote sommen geld beloofd, soms bevat het een verdrietig verhaal en soms gaat het om viruswaarschuwingen waarin u wordt aangespoord een computerbestand te verwijderen. Deze e-mail gaat meestal gepaard met een oproep de e-mail naar zoveel mogelijk mensen door te sturen. Op www.digibewust.nl vindt u hoe u een hoax kunt herkennen en wat u ertegen kunt doen.

VEILIG E-MAILEN TIPS

- Wees voorzichtig met het openen van e-mails van onbekende personen.
- Wees voorzichtig met het openen van attachments. Scan deze eerste met een virusscanner.
- Reageer nooit op spam en verwijder deze direct.
- Installeer een spamfilter of maak gebruik van de mogelijkheden die uw provider biedt. Meld ongewenste e-mail bij **www.spamklacht.nl**.
- Wees voorzichtig met het achterlaten van uw e-mailadres op internet.
- Gebruik meerdere e-mailadressen. Geef uw belangrijkste e-mailadres alleen aan betrouwbare personen en gebruik een makkelijk te vervangen e-mailadres als u een partij (persoon of instantie) niet helemaal vertrouwt.

HELP UW KIND TIPS

- Vertel uw kind geen e-mails te openen van onbekende personen en voorzichtig te zijn met het openen van attachments.
- Vraag uw kind u te vertellen wanneer hij/zij ongewenste e-mail / spam ontvangt. U kunt vervolgens melding maken van deze ongewenste e-mail via **www.spamklacht.nl**.
- Vertel uw kind nooit zomaar ergens zijn/haar e-mailadres in te vullen.
- Vertel uw kind nooit op spam of andere ongewenste e-mail te reageren.

Meer tips? Kijk op www.digibewust.nl

Surfen

Over het internet surfen is een ideale manier om informatie te vinden en bekend te raken met internet. Het springen van webpagina naar webpagina is soms een ware ontdekkingstocht! Maar blijf alert. Want tijdens het surfen kan uw computer zonder dat u dat in de gaten heeft met spyware geïnfecteerd worden of kunt u in aanraking komen met sites waarvan de inhoud u niet aanstaat.

WAAR U OP MOET LETTEN

Omdat u vaak niet weet waar u terecht komt bij het surfen kan het gebeuren dat u op een site komt met **illegale, ongewenste of schadelijke content** (zoals pornografisch, racistisch of gewelddadig materiaal) of dat een **pop-up** met inhoud/reclame waar u niet op zit te wachten in uw scherm verschijnt.

In principe bepaalt u zelf welke **persoonlijke informatie** u wel en welke informatie u niet op internet ter beschikking stelt. Wanneer u gegevens achterlaat op internet is het mogelijk dat kwaadwillende personen hier misbruik van maken door u bijvoorbeeld ongewenst reclame te sturen, uw gegevens door te verkopen, beelden van u ongewenst verspreiden. Uw **privacy** wordt hierdoor aangetast.

Tijdens het surfen kan zonder dat u het weet **spyware** op uw computer geplaatst worden. Deze software kan vervolgens gegevens doorsturen (bijvoorbeeld naar adverteerders) over uw koopgedrag op internet of de websites die u bezoekt. Maar er bestaat ook spyware die op zoek gaat naar uw bank- en creditcardgegevens. Op www.digibewust.nl leest u hoe u spyware kunt tegengaan.

VEILIG SURFEN TIPS

- Verhoog de standaard veiligheids- en privacy-instellingen van uw browser (een **browser** is een programma waarmee u pagina's (websites) op internet kunt bekijken, zoals Internet Explorer of Firefox).
- Wees voorzichtig met het verstrekken van persoonlijke gegevens. Ga van te voren na of de ontvanger van de gegevens betrouwbaar is en of deze de gevraagde gegevens echt nodig heeft.
- Installeer een pop-up killer om het automatisch openen van (reclame)schermen tegen te gaan.
- Installeer anti-spyware software en houd deze up to date.
- Meld websites die niet door de beugel kunnen bij de aangewezen meldpunten, bijvoorbeeld Meldpunt Discriminatie Internet (**www.meldpunt.nl**) en meldpunt Kinderporno (**www.meldpunt-kinderporno.org**).

HELP UW KIND TIPS

- Bereid uw kind voor op wat hij/zij kan tegenkomen tijdens het surfen: ongewenste inhoud van websites, porno, gewelddadige beelden.
- Blijf betrokken bij wat uw kind op internet doet. Is uw kind jong? Surf dan bijvoorbeeld samen met hem/haar. Heeft u een tiener? Toon intresse in wat hij/zij op internet doet en vraag ernaar.
- Maak bij jonge kinderen duidelijke afspraken over internetgebruik en tijdsduur.
- Zet de computer bij voorkeur in het zicht, bijvoorbeeld in de huiskamer.
- Installeer een internetfilter om uw kind tegen ongewenste inhoud van websites te beschermen. Realiseert u zich daarbij wel dat dit met name voor oudere kinderen slechts beperkte bescherming biedt. Zij weten een filter snel te omzeilen. Kijk op **www.digibewust.nl** voor verschillende (gratis) filters.

Meer tips? Kijk op www.digibewust.nl

Downloaden en delen

Via het internet kun u muziek, films, foto's en andere bestanden naar uw eigen computer toehalen. U bent dan aan het downloaden. Ook kunt u zelf via internet bestanden beschikbaar stellen voor anderen. U kunt hiervoor gebruik maken van speciale netwerken: *peer-to-peer-netwerken* of *file-sharing netwerken*. U bent dan bestanden aan het delen. Om aan te sluiten bij zo'n netwerk heeft u wel speciale software nodig die u kunt downloaden via de website van het netwerk.

WAAR U OP MOET LETTEN

Het is volgens de **Nederlandse wet** niet toegestaan zonder toestemming auteursrechtelijk beschermde werken aan te bieden. Dat betekent dat u films, teksten, muziek, en dergelijke die u niet zelf gemaakt heeft niet via het internet aan anderen ter beschikking mag stellen, behalve als de licentie dat expliciet toelaat. U mag natuurlijk wel **eigen werk** aanbieden via file-sharing netwerken.

Wanneer u downloadt via een file-sharing programma wordt het bestand dat u binnenhaalt vaak automatisch ter beschikking gesteld aan anderen (via uw 'shared media folder'). Op dat moment wordt u ook aanbieder van het bestand en dat is niet toegestaan. Sla het gedownloade bestand dus ergens anders op.

U mag voor **eigen gebruik** kopieën maken van muziek of films. Eigen gebruik betekent dat u letterlijk een kopie voor uzelf maakt en deze alleen zelf gebruikt. In dit geval mag u dus films en muziek van internet downloaden, ook als de bron illegaal is.

Software en games zijn extra beschermd. Deze mag u niet voor eigen gebruik downloaden, tenzij u toestemming heeft van de makers. Dat is bijvoorbeeld het geval bij **freeware** en **shareware**.

Ook mag u vrijuit gebruik maken van werken die tot het zogenaamde **publieke domein** behoren. Dat kunnen nieuwe werken zijn waarvan de maker heeft aangegeven dat ze vrij beschikbaar zijn, boeken waarvan de schrijver meer dan 70 jaar geleden is overleden of films, tv-series en concerten die meer dan 50 jaar geleden zijn opgenomen.

File-sharing programmatuur kan deuren naar uw computer openzetten waardoor vormen van **spyware** en **virussen** makkelijker toegang hebben tot uw computer. Ook bevatten bestanden op filesharing netwerken vaak virussen of andere ongewenste software. Hierdoor kan het gebeuren dat uw computer niet goed meer functioneert, maar het is ook mogelijk dat u anderen toegang geeft tot privacygevoelige gegevens op uw computer.

VEILIG DOWNLOADEN EN DELEN TIPS

- Let op de *wet- en regelgeving* op het gebied van auteursrecht op bestanden en media die over het internet heen gaan. Wat u wel en niet mag volgens de Nederlandse wetgeving staat hiernaast beschreven.
- Installeer een *firewall*, een *virusscanner* en *anti-spyware software* en houd deze up to date. Kijk regelmatig of er updates en nieuwe versies beschikbaar zijn op de websites van de leveranciers.
- Met sommige *file-sharing* programma's wordt spyware meegeleverd. Let dus op welk programma u gebruikt.
- Ga ook eens op zoek naar legale muziek op het internet! Veel sites bieden legale muziek, films en andere bestanden te koop of gratis aan via het internet. Deze websites zijn vaak veilig en garanderen een bepaalde kwaliteit. Maar de bestanden zijn vaak op de een of andere manier beveiligd, waardoor de gebruiksmogelijkheden begrensd zijn. Lees van tevoren wat u met de gedownloade bestanden kunt doen.
- Er wordt van alles aangeboden via file-sharing. Ook bestanden die de naam hebben van een bekende film kunnen iets heel anders bevatten. Wees hier op voorbereid.

HELP UW KIND TIPS

- Vraag aan uw kind waar en wat hij/zij downloadt en welke bestanden het uitwisselt.
- Het begrip auteursrecht is moeilijk uit te leggen aan iemand die gewend is alles gratis van internet af te plukken. Maar laat uw kind het eens vanuit een andere invalshoek bekijken. Zou hij/zij het leuk vinden wanneer een foto waar hij/zij veel moeite voor heeft gedaan, door iedereen gratis te gebruiken is?
- Spreek bijvoorbeeld af dat downloaden of installeren alleen mag in uw aanwezigheid. Of dat muziek en spelletjes uit een betrouwbare bron wel, maar gehackte software en illegale muziek niet mogen.

Meer tips? Kijk op www.digibewust.nl

Online kopen en verkopen

Steeds meer mensen kopen hun spullen op internet, variërend van CD's, boeken, kleding en elektronica tot complete reizen. Via internet kunt u zich gemakkelijk oriënteren, prijzen vergelijken, informatie verzamelen en bestellingen plaatsen. Ook online veilingen en tweedehands verkoopsites zijn erg populair. Daar kunt u niet alleen spullen van anderen kopen maar ook uw ook eigen spullen te koop aanbieden. Met een aantal eenvoudige maatregelen beperkt u mogelijke risico's van online kopen en verkopen als het niet, incompleet of beschadigd geleverd krijgen van gekochte artikelen of het niet betaald krijgen van verkochte spullen.

WAT U MOET WETEN

Een **webwinkel** is een omgeving op het internet waar u online producten kunt bekijken en bestellen. Naast winkels die alleen via internet verkopen, bieden ook steeds meer traditionele winkels hun producten aan via internet.

Op **veiling- en advertentiesites** kunt u zelf ook uw spullen aanbieden. En u kunt kijken of iets (antiek, curiosa of andere artikelen) waar u naar op zoek bent voor een lage prijs (al dan niet tweedehands) wordt aangeboden. Voorbeelden van veilingsites zijn *eBay.nl* en *Ooop.nl*. Bekende advertentiesites zijn *Marktplaats.nl*, *Speurders.nl* en *2ehands.nl*.

Net als bij de aankoop van een product in de gewone winkel heeft u bepaalde rechten bij het online kopen van producten. Zo staat er in **de wet** dat u een via internet gekocht product (niet van een particulier) binnen zeven dagen mag retourneren en uw geld daarvoor terugkrijgt. Er zijn echter wel een aantal uitzonderingen, zoals bij producten die speciaal op maat zijn gemaakt of die snel kunnen bederven of verouderen. Ook moet de verkopende partij aan bepaalde eisen voldoen, zoals het verstrekken van zijn identiteitsgegevens, de belangrijkste productgegevens, de leveringsvoorwaarden, de wijze van betaling en de garantievoorwaarden.

VEILIG ONLINE KOPEN EN VERKOPEN TIPS

VEILIG ONLINE KOPEN

- Vraag u af wie er achter de webwinkel zit. Iedere webwinkel moet contactgegevens op de website zetten.
- Is de webwinkel duidelijk over de kwaliteit van de producten, de garantie, de service, de leveringsvoorwaarden, bijkomende verzendkosten, enzovoort?
- Bewaar een kopie en/of print van uw bestelling, de orderbevestiging, e-mailcorrespondentie en alle voorwaarden voor het geval er iets mis mocht gaan.
- Vraag een vast telefoonnummer en/of woonadres van de verkoper die via de veiling- of advertentiesite zijn producten aanbiedt. Deze gegevens kunt u op echtheid controleren via bijvoorbeeld www.detelefoongids.nl.
- Sommige websites zijn voorzien van een keurmerk waaraan gedragsregels voor verkopen via het internet verbonden zijn. Het bekendste Nederlandse keurmerk is het Thuiswinkel Waarborg (**www.thuiswinkelwaarborg.nl**).

VEILIG ONLINE VERKOPEN

- Schrijf volledige advertentieteksten, met daarin opgenomen een beschrijving van eventuele beschadigingen aan het product. Zorg voor goede foto's. Zo voorkomt u dat een koper teleurgesteld raakt in het product dat u levert.
- Zorg ervoor dat u betrouwbaar overkomt: laat u verifiëren of controleren door de site waar u uw product te koop aanbiedt.
- Maak duidelijke afspraken over leverings- en betaalvoorwaarden. Wie neemt bijvoorbeeld de transportkosten voor zijn rekening?
- Vraag een koper altijd om zijn adresgegevens en een (vast) telefoonnummer. Deze gegevens kunt u op echtheid controleren via bijvoorbeeld www.detelefoongids.nl.
- Als de koper het verkochte artikel per post wenst te ontvangen, verstuur het artikel dan niet voordat u het verkoopbedrag op uw bankrekening heeft staan.

Meer tips? Kijk op www.digibewust.nl

Online betalen

Betalen op internet voor online bestelde producten of diensten is geen probleem, zolang zowel koper als verkoper zorgvuldig met de klantgegevens omgaan en gebruikmaken van de beveiligingsmogelijkheden die internet biedt. Dit betekent dat u net als in de 'off-line' wereld kritisch moet kijken naar de mogelijkheden en de veiligheid van betalen via internet.

WAT U MOET WETEN

Er zijn **diverse online betaalmethoden** die u bij het kopen van producten op internet tegen kunt komen. U kunt online betalingen verrichten met *creditcard, digitale acceptgiro*, of via uw *eigen bankrekening*. Er bestaan ook diverse systemen voor kleine betalingen (*'micro payments'*).

U kunt daarnaast vaak gebruikmaken van de klassieke methoden, zoals de acceptgiro of onder rembours. Maak hierin uw eigen afweging. Houd daarbij rekening met zaken als de veiligheid van de betaalmethode, de betrouwbaarheid van de leverancier, de betaalopties die de leverancier biedt en het gebruiksgemak en de kosten van de betaalmethode.

Achteraf betalen komt veel voor bij internetwinkels die zijn voortgekomen uit postorderbedrijven. Hierbij betaalt u het artikel nadat u het heeft gekregen en goed heeft bevonden. Als het niet goed is stuurt u het per post weer terug en hoeft u niets te betalen. Bij de grootste groep winkels op internet moet u echter vooraf betalen om uw aankoop thuisgestuurd te krijgen.

Bij online betalen is het belangrijk dat de betaling via een **beveiligde verbinding** plaatsvindt. Uw gegevens (bijvoorbeeld creditcardgegevens) worden dan versleuteld, zodat niemand anders op internet deze gegevens kan zien of kan volgen. Een aanwijzing om te weten of een betaling beveiligd plaatsvindt kunt u vinden in de adresregel (URL) van de website. Deze begint met https in plaats van http. Ook kunt u een beveiligde verbinding herkennen aan het gesloten slotje of sleuteltje onder in het scherm.

VEILIG ONLINE BETALEN TIPS

- Controleer of de betaling via een beveiligde verbinding plaatsvindt: begint de adresregel met https? Is er onder in het scherm een gesloten slotje of sleuteltje zichtbaar?
- Lees de privacyvoorwaarden, de leveringsvoorwaarden en de betaalvoorwaarden voordat u tot betalen overgaat.

Meer tips? Kijk op www.digibewust.nl

Online bankieren

Veel mensen regelen tegenwoordig hun bankzaken via internet. U hoeft geen rekening meer te houden met de openingsuren van de bank en u hoeft niet meer te wachten aan het loket. U regelt gewoon alles zelf vanachter uw computer. Banken voldoen aan strenge beveiligingsstandaarden voor elektronisch betalingsverkeer. Maar u kunt zelf ook bepaalde maatregelen nemen om het online bankieren nog veiliger te maken.

WAT U MOET WETEN

Banken nemen allerlei (technische) **beveiligingsmaatregelen** om ervoor te zorgen dat alleen u toegang heeft tot uw bankrekeningen. Zij gebruiken bijvoorbeeld een beveiligde verbinding die ervoor zorgt dat alle gegevens tussen uw computer en de computer van de bank worden versleuteld. Daardoor zijn uw gegevens alleen leesbaar voor de computer van de bank. De beveiligde verbinding is te herkennen aan het gesloten hangslotje onder in het scherm. Daarnaast heeft iedere bank een identiteitscontrole. U krijgt alleen toegang tot uw rekeningen via geheime codes vaak in combinatie met uw pincode.

Belangrijk is om uw **wachtwoorden** en codes (van uw computer, e-mail en andere digitale middelen) strikt persoonlijk te houden. Bewaar deze dan ook niet op of in de buurt van uw computer of andere gangbare plaatsen (agenda en dergelijke) en vertel ze nooit aan iemand anders. Kies voor niet voor de handliggende maar wel enigszins eenvoudig te onthouden wachtwoorden met minimaal 8 karakters (zowel letters, cijfers als leestekens), bijvoorbeeld 'VlaFlip!59'. Op **www.digibewust.nl** staan tips voor het verzinnen van een veilig wachtwoord.

Een van de gevaren van online bankieren is **phishing** (zie ook p. 10). Dit is een vorm van oplichting via internet waarbij een oplichter uw creditcardnummer of pincode probeert te achterhalen. Een e-mail met het verzoek uw gegevens ergens in te voeren, lijkt dan bijvoorbeeld van uw bank te komen. Uw bank zal u echter nóóit via de e-mail naar dit soort gegevens vragen. Op **www.digibewust.nl** leest u hoe u phishing e-mails en phishing websites kunt herkennen.

Keylogging is een andere manier die door kwaadwillenden gebruikt wordt om achter persoonlijke gegevens te komen. Dit is *spyware* die de toetsaanslagen van uw toetsenbord registreert en doorstuurt. Zo kan deze software achter wachtwoorden, rekeningnummers en creditcardgegevens komen.

VEILIG ONLINE BANKIEREN TIPS

- Installeer een *firewall, anti-spyware software* en een *virusscanner* op uw computer en houd deze up to date.
- Controleer of u via een veilige verbinding met uw bank communiceert: begint de adresregel met https? Is er onder in het scherm een gesloten slotje of sleuteltje zichtbaar?
- Ga niet in op e-mails waarin wordt gevraagd naar uw rekeningnummer/creditcardnummer of pincode ook al lijken deze afkomstig van uw bank- of creditcardmaatschappij. Uw bank- of creditcardmaatschappij zal namelijk nooit via de e-mail naar deze gegevens vragen.
- Kies een veilig wachtwoord en ga er veilig mee om. Zie ook **www.digibewust.nl**.
- Check de website van uw eigen bank voor meer informatie over welke maatregelen uw bank neemt en hoe zij u kunnen helpen bij problemen.
- Op **www.veiligbankieren.nl** vindt u meer informatie over wat de bank doet om u veilig online te laten bankieren en wat u zelf kunt doen.

Meer tips? Kijk op www.digibewust.nl

Gamen

Gaming is erg populair, onder jong en oud. Via spelcomputers (zoals de Xbox 360, DS, Wii en PSP) kunt u schietspellen, strategische spellen, sportspellen, simulatorspellen en adventure games spelen. U kunt ook online gamen, alleen of juist met andere spelers over de hele wereld. Online games lopen uiteen van bijvoorbeeld online pokerspellen tot belevenissen in virtuele of fantasiewerelden.

WAT U MOET WETEN

Er zijn diverse soorten games. Ook spellen die geproduceerd of gebruikt worden voor een ander doel dan alleen vermaak, namelijk om bepaalde vaardigheden te leren of kennis en inzicht op te doen. Een voorbeeld is Gebouw 13 van Digibewust (**www.gebouw13.nl**) waar kinderen tussen de 8 en 14 jaar spelenderwijs kennismaken met de mogelijkheden, kansen maar ook risico's van internet.

Een bekende en veel voorkomende online game is de *"massive multi-player online role-playing game"* of **MMORPG**. Dit is een spel waarbij u met duizenden mensen tegelijkertijd in een virtuele wereld problemen of raadsels oplost of vecht tegen andere spelers. Voor de meeste MMORPG's moet je maandelijks een bedrag betalen voor een abonnement. Bekende voorbeelden van MMORPG zijn *World of Warcraft* en *Everquest*. Ook *Second Life* is een MMORPG maar dan zonder spelelement.

In online games zit vaak de mogelijkheid met elkaar te chatten of contact te zoeken. Het kan gebeuren dat u via deze kanalen berichten met schadelijke inhoud ontvangt, zoals scheldberichten.

In sommige online spellen kunnen spelers allerlei rijkdommen vergaren, zoals speciale wapens of virtueel geld. Die kunnen rechtstreeks of via veilingwebsites worden ingewisseld voor echt geld. Via *spyware* kunnen kwaadwillenden inloggegevens ontfutselen en u **beroven van uw virtuele eigendommen**.

VEILIG GAMEN TIPS

- Installeer een *firewall*, een *virusscanner* en *anti-spyware software* en houd deze up to date door regelmatig te kijken of er updates en nieuwe versies beschikbaar zijn op de website van de leveranciers.
- Wees bedacht op berichten van uw medespelers waar u niet op zit te wachten.
- Kies een veilig wachtwoord om in te loggen in een game en ga er veilig mee om. Op **www.digibewust.nl** staan tips voor het verzinnen van een veilig wachtwoord.
- Neem rustpauzes tijdens het spelen van een game, zorg dat u regelmatig drinkt en beweegt tijdens het spelen van een game.
- Zorg ervoor dat gamen niet uw enige (vrije) tijdsbesteding is. Stel grenzen aan uw eigen gamen.

HELP UW KIND TIPS

- Speel samen met uw kind of kijk met hem/haar mee en praat over de games.
- Zet de (spel)computer bij voorkeur in het zicht, bijvoorbeeld in de huiskamer.
- Maak vergelijkingen tussen situaties in games en in de werkelijkheid. Wat kan helemaal niet en wat kan wel? Wat is echt en wat is nep?
- Spreek tijden af wanneer en hoe lang uw kind mag gamen.
- Kijk voor aankoop of een spel geschikt is voor uw kind via **PEGI online**, de Kijkwijzer voor games. De PEGI symbolen geven daarnaast ook indicatie over de inhoud. Zie ook **www.weetwatzegamen.nl**.

Meer tips? Kijk op www.digibewust.nl

Mobiel bellen

De mobiele telefoon is niet meer weg te denken uit ons dagelijks leven. Bijna iedereen heeft er een en lang niet meer alleen om mee te telefoneren. Surfen, e-mailen, fotograferen, filmen, SMS'en, MMS'en, muziek beluisteren en spelletjes spelen zijn de nieuwe functionaliteiten van een modern mobieltje. Met niet in de laatste plaats een enorme aantrekkingskracht op kinderen en tieners. Juist omdat er steeds meer kan met een mobiele telefoon is het zaak er ook verstandig en veilig mee om te gaan.

WAT U MOET WETEN

Een **SMS** (Short Messaging Service) is een tekstberichtje dat zowel wordt verstuurd via de mobiele telefoon als daar ook op binnenkomt. **MMS** (Mulitimedia Messaging Service) zijn berichten die naast tekst ook beeld, geluid en film kunnen bevatten.

Het kan gebeuren dat u via SMS/MMS ongevraagde reclameberichten (**SMS-spam**) ontvangt. Vaak zijn deze berichten persoonlijk gemaakt. Spammers komen aan mobiele nummers doordat mensen deze bijvoorbeeld achterlaten op websites voor het ontvangen van een ringtone of ander mobiel vermaak.

Het komt gelukkig (nog!) niet vaak voor, maar ook uw mobieltje kan besmet raken met een virus. Net als bij een computer zit er in een mobiele telefoon een besturingssysteem dat geïnfecteerd kan raken met een **virus**: een softwareprogrammaatje dat uw telefoongegevens vernielt. Een virus komt bijvoorbeeld vermomd als spelletje dat u heeft gedownload op uw mobieltje terecht.

Er bestaan allerlei **diensten voor het mobieltje:** het per SMS ontvangen van het weerbericht, sportuitslagen of horoscoop en het aanvragen van ringtones. Lang niet altijd gaat het om een eenmalig koop, maar blijkt het een abonnementsvorm te zijn. Het gebruik van deze diensten kan daardoor duur worden. In Nederland worden aanbieders van SMS-diensten geacht zich te houden aan de gedragscode voor SMS-diensten. Hierin staat bijvoorbeeld dat in reclame-uitingen informatie moet worden gegeven over kosten en frequentie. Overigens kunt u op de website van uw mobiele provider een overzicht vinden van aanbieders van SMS-diensten met contactgegevens en afmeldprocedure.

De meeste mobieltjes zijn voorzien van een camera waarmee u foto's en **filmpjes** kunt maken. Deze kunt u vervolgens ook doorsturen naar andere mobieltjes (via MMS of Bluetooth) of op een website plaatsen. Maar mensen kunnen ook ongewenst foto's of filmpjes van anderen maken en deze via internet verspreiden. Een voorbeeld is **happy slapping**: het maken van filmpjes van een willekeurige persoon die in elkaar wordt geslagen en deze vervolgens op internet plaatsen.

VEILIG MOBIEL BELLEN TIPS

- Wees voorzichtig met het geven van uw mobiele nummer.
- Neem voor online activiteiten via de mobiele telefoon dezelfde voorzorgsmaatregelen als voor de computer.
- Lees goed de voorwaarden voordat u een mobiele dienst koopt: wat zijn de kosten? Gaat het om eenmalige kosten of om een abonnement? Kunt u de dienst makkelijk stopzetten?
- Reageer niet op SMS of MMS van onbekende afzenders.
- Download geen spelletjes, ringtones of andere bestanden van sites die u niet vertrouwt. De mogelijkheid bestaat dat u daarmee een virus binnenhaalt.

HELP UW KIND TIPS

- Hoe meer u zich voor het mobiele telefoongebruik van uw kind interesseert, hoe beter u daarover met hem/haar kunt praten. Laat uw kind bijvoorbeeld uitleggen hoe een functionaliteit op de mobiele telefoon werkt.
- Spreek regels af over het gebruik van het mobieltje: wie betaalt de rekening? Hoe kan diefstal voorkomen worden? Moet uw kind om toestemming vragen wanneer hij/zij bijvoorbeeld gebruik wil maken van een SMS-dienst?
- De mobiele telefoon is voor tieners een belangrijk communicatiemiddel. Verbieden ervan is dus een zware straf. Zoek samen naar oplossingen bij misbruik of problemen.

Meer tips? Kijk op www.digibewust.nl

Woordenlijst

WOORDENLIJST

MEER INFORMATIE

Wilt u meer informatie of tips over de in deze uitgave genoemde onderwerpen? Kijk dan op **www.digibewust.nl**. Hier vindt u ook tips over veilig internetten voor ouders, docenten en het MKB.

Deze uitgave kunt u bestellen via *info@digibewust.nl*

COLOFON

Dit is een uitgave van Digibewust. Digibewust is een samenwerkingsverband tussen overheid en bedrijfsleven om het veilig gebruik van internet en andere digitale middelen bij mensen te vergroten.

Teksten en redactie:
Inge Aarts, Digibewust

Contact:
Overgoo 11, 2260 AG Leidenschendam
tel 070-4190309 • fax 070-4190650
www.digibewust.nl • info@digibewust.nl

Grafische vormgeving:
Maarten Kuijt, Dune Reclamebureau

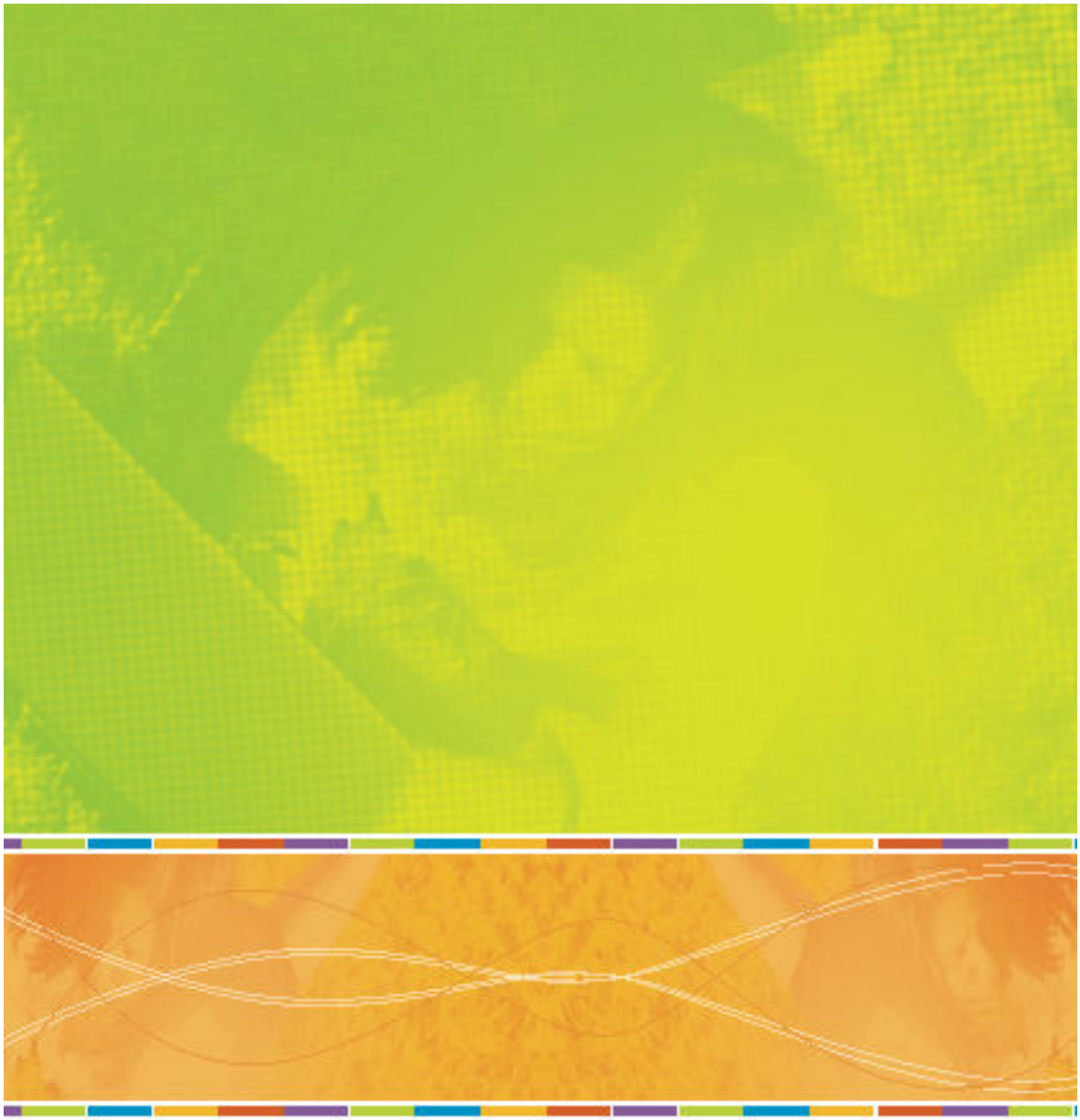
Druk:
Efficiënta Offset drukkij bv

PARTNERS:

HOOFDSPONSOR:

COALITIEPARTNERS:

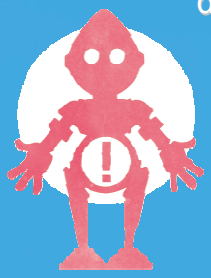
Notities



Bijlage 2: jongerengids 'Als een visje door het net'

TIP: "IK SURF, DUS IK SPORT?"

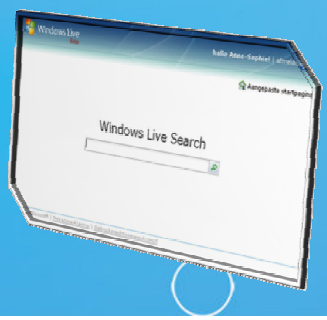
Net als een watersurfer van de ene golf op de andere springt, kan je op het internet eenvoudig van de ene pagina naar de andere dwalen door op hyperlinks te klikken. Vandaar dus de term 'websurfen'. Je kunt rondsurfen omdat je iets opzoekt voor school, maar dit kan evengoed voor je hobby zijn. Het leuke aan surfen is dat je telkens nieuwe sites ontdekt!



TIP: "LOST IN CYBERSPACE?"

Vind je niet wat je zoekt ? Probeer deze trucjes met Live.com!

- Zet het teken '&' tussen je zoekwoorden: Je vindt dan alle pagina's die de woorden bevatten die jij ingeeft.
  - Bijv. hond & kat
- Zet je zoekwoorden tussen dubbele aanhalingstekens: Je vindt die pagina's met de exacte woorden die je opgeeft.
  - Bijv. "virtuele wereld"
- Typ 'filetype:' gevolgd door het soort bestand dat je zoekt: Zo vind je webpagina's met een specifiek bestandstype.
  - Bijv. informatie filetype:doc (voor een Word-bestand)
  - Bijv. huiswerk filetype:pdf (voor een PDF-bestand)



TIP: "EFFICIËNT ZOEKEN ONLINE?"

- Zoeken per categorie: de resultaten zijn beschikbaar per type informatie zoals internet pagina's, beelden en actualiteit.
  - Weten wat er in de wereld gebeurt? Typ je zoektermen in de zoekrobot in en klik vervolgens op 'Nieuws'.
  - Een foto voor je huiswerk? Typ de zoektermen in de zoekrobot in en klik vervolgens op 'Beelden'
- De zoom-functie: de zoekrobot biedt de mogelijkheid om meer of minder gedetailleerd te zoeken met behulp van een schuivertje dat heel eenvoudig te bedienen is.

Op www.clicksafe.be vind je een heleboel info over dingen die niet kunnen op het internet. Bij Child Focus kan je terecht met vragen over kindermisbruik. Ook de politie heeft een speciale 'Federal Computer Crime Unit' (FCCU) die computermisdaden en kindermisbruik bestrijdt. Blijf dus niet zitten met je probleem!

TIP: "S.O.S. KINDERMISBRUIK"

- Wil je iets melden aan de internetpolitie FCCU? Stuur dan een email dan naar contact@fccu.be.
- Child Focus kan je gratis bellen op het nummer 110, zelfs anoniem!
- Of surf naar www.clicksafe.be.

Kunnen mijn ouders zien op welke websites ik geweest ben?

Ja, alle websites die jij bezoekt, zijn te zien met een klik op de geschiedenisknop van je surfprogramma (= de 'browser', bijv. Internet Explorer). Beter nog is de applicatie Windows Live OneCare Parent Controle, waarbij je samen met je ouders de sites - en de inhoud ervan - waartoe je toegang hebt, kan kiezen.

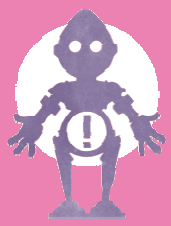
Net zoals in het echte leven heb je ook op het internet een adres nodig om post te krijgen. Dat adres bestaat uit een naam, een apenstaartje @ en de naam van degene die jouw elektronische post verstuurt (bijv. Hotmail). Je moet ook een paswoord kiezen zodat niet iedereen je mails kan lezen. Surf gewoon naar zo'n site met een e-maildienst, volg de verschillende stappen en mailen maar!

TIP: "E-MAILADRES UNDERCOVER!"

Zo heb je een veilig e-mailadres in geen tijd:

Wees origineel! Gebruik niet zomaar je voornaam of familienaam in je adres, want dan maak je het anderen te makkelijk om je op te sporen.

Een wachtwoord dat niet te kraken valt, krijg je zo:



- Combineer kleine en grote letters met cijfers en symbolen.
- Maak een afkorting van een zin die je gemakkelijk kan onthouden.
- Laat de klinkers weg uit je favoriete uitspraak.

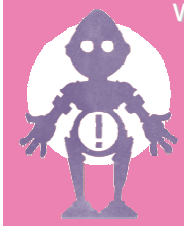
MSN Hotmail (www.hotmail.be) checkt automatisch de veiligheid van je paswoord als je een nieuw adres aanmaakt.

Hoe hou je ONGEWENSTE? mails uit je inbox

Mail die je eigenlijk niet wil, wordt 'spam' genoemd. Eigenlijk is het woord een merknaam van ingeblikt varkensvlees (SPiced hAM). Het kreeg vooral bekendheid door de komische show van Monty Python, waarin het blikjesvlees de hemel wordt ingeprezen. Spam in je mailbox kan knap vervelend zijn, want het gaat vaak om reclame. Om minder spam te krijgen zijn er enkele simpele regels: geef je e-mailadres nooit zomaar door op het internet en antwoord niet op ongewenste mails! Zo weten de afzenders immers dat jij hun berichten leest en gaan ze gewoon door. Maak ook verschillende e-mailadressen aan, bijv. één voor school en één voor de fun! Neem bovendien een goede e-maildienst met spamfilter, zoals Hotmail.

TIP: "CAMOUFLEER JE STAARTJE!"

- Wil je je e-mailadres toch op je eigen webpagina of blog plaatsen? Vervang '@' dan door 'at' (bijv. ollieathotmail.com i.p.v. ollie@hotmail.com). Zo ben je de spammailers te slim af! Als je een formulier moet invullen en doorsturen, is je juiste adres mét apenstaartje wel nodig, anders krijg je een foutmelding. Straks meer over weblogs.

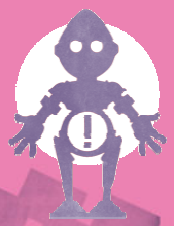


Waarom zijn sommige mails ook GEVAARLIJK?

In sommige mails kan een computervirus zitten dat je hele computer doet flippen. Verwijder mails van onbekenden daarom best direct en open zeker nooit een rare bijlage. Je hoeft ook nooit te antwoorden op mails die je niet vertrouwt. Betrouwbare bedrijven vragen nooit info via mail.

Wat kan je doen als je GEPEST? *wordt via mail*

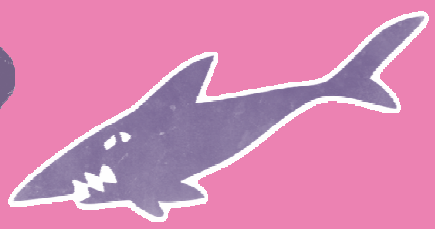
Blokkeer die pestkop in je inbox! Blijft hij of zij je lastigvallen? Maak dan een nieuw e-mailadres aan en geef het alleen aan je beste vrienden. Om de pesters te vinden, heb je bewijsmateriaal nodig. Bewaar de pestmails of print ze uit (hoe erg ze ook zijn) en ga ermee naar je ouders of leerkracht.



TIP: "HOU INDRINGERS BUITEN!"

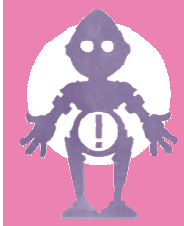
Wil je enkel mails krijgen van je vrienden uit je adresboek? Bij MSN Hotmail kan dat! Klik op 'Instellingen', dan op e-mail en ten slotte op 'Bescherming tegen spam'. Kies de optie 'Exclusief' bij 'Niveau van de spamfilter'. Zo krijg je enkel nog mails van leuke vrienden! Je kan altijd je andere e-mails zien bij 'Ongewenste e-mail'.

Wat is PHISHING?



'Phishing' wordt gebruikt wanneer oplichters op het internet proberen te 'vissen' naar persoonlijke info zoals paswoorden, codes, adressen…waarmee ze dan bijv. geld van je rekening halen. Ze doen dit door e-mails te versturen die verdacht veel lijken op een mail van je bank of een andere belangrijke organisatie. De oplichters leiden je naar een valse website waar jij, je van geen kwaad bewust, allerlei info vrijwillig invult. Geef je privé-gegevens dus nooit zomaar vrij op het internet.

TIP: "DE ENE VIS IS DE ANDERE NIET!"



Bij 'phishing' draait het duidelijk om het 'vissen' naar vertrouwelijke gegevens in de zee van internetgebruikers. Waarom schrijven we dan niet gewoon 'fishing'? Dit is geen schrijffout, maar een gewoonte uit de hackerswereld. Deze computerinbrekers vervangen vaak de letter 'f'' door 'ph'. Daarmee verwijzen ze naar de eerste vorm van hacking, 'phone phreaking': in de jaren '70 werden telefooncentrales met speciale tonen gemanipuleerd, waardoor de hacker gratis of op andermans kosten kon bellen.

PC-WEETJE

Mijn broer en zus gebruiken ook mijn pc. Hoe zorg ik ervoor dat ze van mijn gegevens afblijven?

Jullie kunnen dit vermijden door verschillende 'gebruikersaccounts' aan te maken voor jullie computer. Zo hebben jullie elk een eigen profiel met je eigen documenten, lijst van favoriete websites…Iedereen heeft een eigen paswoord om de computer te kunnen gebruiken, dus niemand kan nog aan de gegevens van de andere! Als je een bezoeker hebt, kan je ook een 'gastaccount' aanmaken. Zo zijn er zeker geen problemen meer met jouw gegevens op de computer!

Wat is een COMPUTERVIRUS?

Net zoals er virussen bestaan die mensen ziek maken, zijn er ook speciale virussen die computers aantasten. Zo'n computervirus is eigenlijk een computerprogramma (gemaakt door mensen!) dat ongemerkt binnensluipt in je computer. Hierdoor zal die raar doen: ofwel werkt hij helemaal niet meer ofwel zie je aan kleine dingen dat er iets mis is. Er zijn dus verschillende soorten virussen.

TIP: "GASTEN ONDER DE SCANNER!"

Installeer zeker een virusscanner op je computer. Zo'n programma controleert alle bestandjes die je opent of afhaalt en haalt de virussen er zo uit! Je moet je virusscanner wel vaak 'updaten' (vernieuwen) zodat hij ook de laatste nieuwe virussen herkent. Updaten kan je doen via de website van je virusscanner. Simpel, en je computer kan er weer tegenaan! Bij het Windows Live OneCare Safety Center kan je je pc makkelijk controleren op virussen.

Hoe krijg ik een VIRUS op mijn computer?

In elk bestandje of programma kan een virus verstopt zitten. Het doorgeven van een virus gebeurt meestal via internet of e-mail (online) of via een CD-ROM of geheugenkaartje (offline). Pas dus altijd op met nieuwe bestanden of programma's.

TIP: "OPGERUIMD STAAT NETJES!"

Als je beveiligingsprogramma toch kwaadaardige software opspoort, dan moet je die enkel door de virusscanner laten verwijderen. Selecteer de bestanden die je niet vertrouwt en volg de richtlijnen om je pc weer tiptop in orde te maken. Vraag de hulp van een kenner of de computerwinkel als dit je petje te boven gaat!

Wat is het verschil tussen een

WORM?

en een gewoon computervirus

Een worm dringt ook je computer binnen, maar verspreidt zichzelf naar andere computers zonder dat jij iets doet. Hij hangt zich niet vast aan een bestand of programma, maar stuurt zichzelf door naar e-mailadressen die hij tegenkomt in je computer.

Waarom is

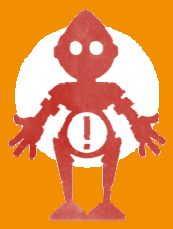
SPYWARE?

niet zo spannend als de naam doet vermoeden

'Spyware' betekent eigenlijk 'spionnensoftware' omdat deze programma's zich stiekem op je computer installeren en info verzamelen over welke sites jij bezoekt. Deze 'spionnen' zorgen er ook voor dat je computer heel wat trager werkt of dat er reclamevenstertjes op je scherm komen, zelfs als je niet surft! Alle info die zo'n programma vindt over jouw surfgedrag kan zelfs worden verkocht aan bedrijven! Surf dus slim en installeer een antispywareprogramma op je pc!

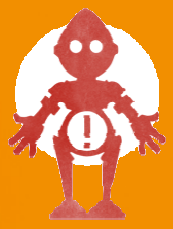
TIP: "WEG MET POP-UPS!"

Pop-ups zijn die vervelende venstertjes met reclame die altijd op je scherm floepen als je surft. Klik ze gewoon weg op het kruisje in de rechterbovenhoek. Een pop-up stopper houdt die venstertjes mooi tegen. Zo'n programma vind je bijvoorbeeld ingebouwd in de werkbalk van Windows Live. Je kunt die gratis downloaden op http://toolbar.live.com.

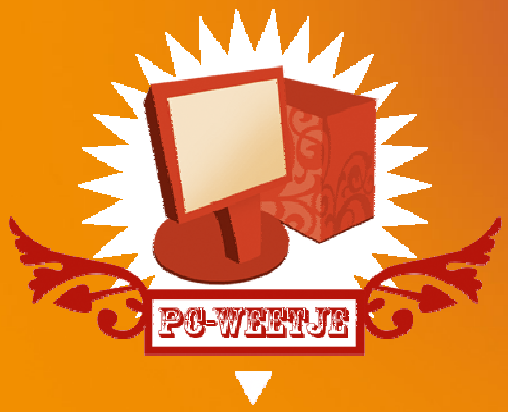


TIP: "KRUIMELS IN JE COMPUTER!"

Ook je computer eet graag koekjes…Maar 'cookies' zijn kleine tekstbestandjes die op je harde schijf belanden na het bezoeken van een website. Deze cookies zorgen dat de website jou de volgende keer herkent en bijv. weet welke taal je kiest. Cookies kunnen ook onthouden wat je allemaal uitspookt op een site en dan toont de site info die jij misschien wel leuk vindt.



Als je geen sporen wil nalaten, verwijder dan je cookies na elke surfbeurt! Bij Internet Explorer klik je in de menubalk op 'Extra', dan 'Internet-opties' en 'Cookies verwijderen'.

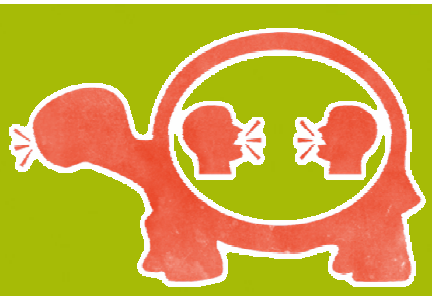


Wat doe ik als mijn computer helemaal niets meer wil doen?

Ai, dat is natuurlijk niet zo leuk…Probeer eens de toetsen Ctrl, dan Alt en Delete. Normaal verschijnt er een schermpje waar je de vastgelopen programma's kan sluiten. Lukt dit niet, druk dan op de Reset-knop van je computerbak. Heb je geen Reset-knop, druk dan heel lang op de startknop. Je computer moet dan uitvallen. Wacht eventjes voor je hem weer aanzet, dan zou alles weer moeten werken. Schakel je ouders of een computerwinkel in als je computer vaak vastloopt.

Wat is het verschil tussen een open en een gesloten

CHATBOX?



Een open chatbox staat gewoon op een website, iedereen kan er chatten. Een gesloten chatbox moet je eerst downloaden op je computer. Jij kiest dan zelf met wie je wil chatten door vrienden toe te voegen aan je contactenlijstje!

TIP: "ZOEK EENS MET TWEE!"

Met Windows Live Messenger kan je veel meer doen dan chatten! Je kan bijvoorbeeld samen iets opzoeken. Je chatvriend kan dan ook alle zoekresultaten zien in het chatvenster. Handig als jullie samen een taak maken!

Voor je scherm durf je meer te

VERTELLEN

dan in het echt, maar is dit wel

ZO SLIM?

Op internet zeg je makkelijker dingen omdat niemand je ziet. Maar je weet natuurlijk nooit wie er meeleest…Blijf dus online gewoon jezelf en doe geen dingen die je anders niet zou doen, zoals je adres of telefoonnummer aan een vreemde geven of mensen pesten. Vergeet niet dat je gesprek door de ander bewaard kan worden…

Wat is het verschil tussen

online en offline

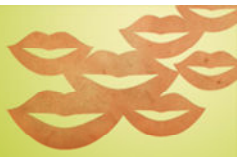
PESTEN?

Ben jij een cyberpestkop? Misschien denk je van niet, maar cyberpesten kan uiteenlopende vormen aannemen. Het kan zijn dat je al beledigende of bedreigende mails hebt verstuurd, een roddel hebt gelanceerd of iemand bewust hebt uitgesloten in een chatprogramma.

Een onschuldig grapje kan gauw uit de hand lopen: online pesten is namelijk nog veel erger dan het 'gewone' pesten:

- Woorden komen hard aan op een scherm en je kunt niet zien hoe de ander reageert.
- Het slachtoffer voelt zich thuis niet meer veilig, het pesten gaat gewoon door na de schooluren.
- Wat online staat, kan je niet meer ongedaan maken. Een bewerkte foto of een beledigende tekst kan verder verspreid worden!

TIP: "CYBERPESTEN GEBEURT NIET ONGESTRAFT!"



Bij ernstige gevallen kan je de politie inschakelen. De Federal Computer Crime Unit grijpt in bij reële bedreigingen en online stalking. Die kunnen al het materiaal op internet traceren, ook al denkt de cyberpestkop dat hij geen sporen achterlaat. Je kunt de FCCU mailen op contact@fccu.be.

Word je zelf gepest, dan verzamel je best zo veel mogelijk bewijsmateriaal, bijv. door de geschiedenis van je chatsessies bij te houden of door een printscreen te maken.

TIP: "SURFEN BINNEN DE LIJNTJES!"

Ja, ook op internet zijn er beleefdheidsregels: 'netiquette'! Saai? Vergeet niet dat jijzelf ook graag correct behandeld wordt.

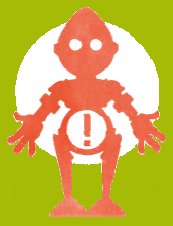
Enkele gouden regels:

•Typen in drukletters is zoals roepen in het echt. Hou het dus rustig en WEES NIET AGRESSIEF ONLINE.

•Respecteer de privacy van anderen. Stuur geen persoonlijke mails of gegevens door zonder hun toestemming.

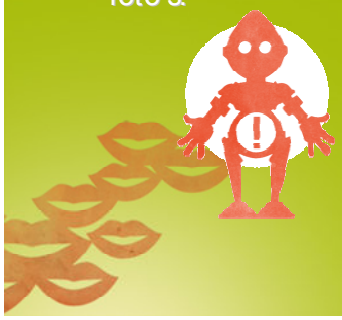
•Pas je toon aan naargelang waar je bent online. Tegen je vrienden praat je anders dan tegen je leraar, ook op internet.

•Denk aan de tijd en de surfsnelheid van anderen. Vind jij het altijd leuk om de zoveelste kettingmail of een superzware bijlage te ontvangen zodat je inbox tilt slaat?



Zijn chatvrienden even BETROUWBAAR? als offline vrienden

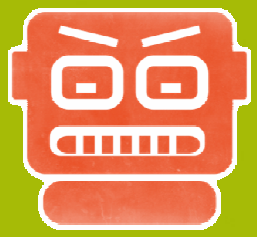
Online heb je zeker ook 'vrienden' die je nog nooit in het echt gezien hebt. Dit kunnen supertoffe mensen zijn, maar je weet natuurlijk nooit zeker wie ze écht zijn. Zo kan een 'leuk meisje' op de chat in het echt een saaie, oude man zijn…Zelfs na 1.000 leuke chats, blijft je chatvriend altijd een onbekende aan wie je beter geen persoonlijke info geeft zoals je telefoonnummer, adres of foto's.



TIP: "DAG VREEMDE!"

Toch zin om een chatvriend te zien? Spreek dan af op een plaats die je goed kent en waar veel mensen zijn. Als je niet op je gemak bent, kan je gewoon weggaan. Vertel het zeker ook aan je ouders of een goede vriend en neem iemand mee.

Wat kan je doen bij VERVELENDE CHATS? of als je tijdens het chatten wordt gepest



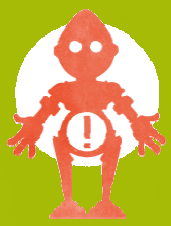
Chatten moet fun zijn! Als je het niet leuk vindt, reageer dan niet meer op nare berichten. Chat met iemand die wel leuk is of log gewoon uit! Stomme chatvrienden kan je ook blokkeren zodat ze jou nooit meer lastigvallen. Vertel het zeker aan je ouders of een goede vriend. Praten helpt!

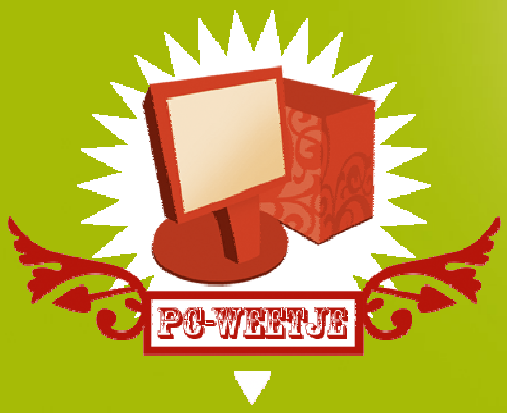
TIP: "RARA, WIE BEN IK?"

Bijnamen of nicknames zijn heel gewoon op internet: om te chatten, te mailen, je mening te geven op forums... Het is gewoon veel leuker om op internet een originele naam te gebruiken! Bedenk een naam zonder persoonlijke info prijs te geven. Zo weet niemand wie je bent en kunnen ze jou in het echt niet vinden!

TIP: "VERBAN DIE CHATVRIEND!"

Geen zin meer in praatjes van een rare chatvriend? Blokkeer hem gewoon! Bij MSN Messenger klik je simpelweg op zijn naam met de rechtermuisknop en kies je 'Blokkeren'. Dan ziet die persoon niet meer wanneer jij online bent en kan hij je niet meer lastig vallen! Wil je hem ook uit je vriendenlijst? Klik dan op 'Verwijderen'. Opgeruimd staat netjes..!

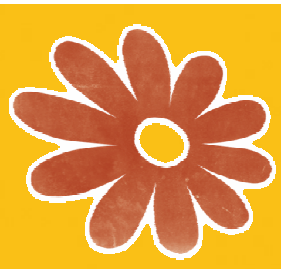




Waarom mag ik van mijn ouders zo weinig doen op internet?

Internet kan heel leuk zijn, maar je vindt er ook rare dingen waartegen je ouders je willen beschermen. Ook kan je computer bijv. een virus oplopen door bestanden van internet. Of misschien zijn je ouders bang dat je te veel op internet zou zitten en je niets anders meer zou doen. Vertel je ouders waarom je op internet wil, toon hen wat je er doet en spreek af hoe lang je per dag op internet mag. Misschien helpt dit wel…

Wat is een WEBLOG?

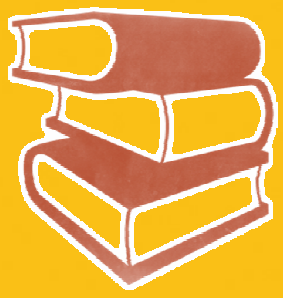


Een weblog of blog is een persoonlijke pagina op internet die vaak vernieuwd wordt. Zonder veel technische kennis kan de schrijver zijn gedachten online delen door tekstjes of foto's te 'posten'. Meestal gaat het over persoonlijke dingen die hij meemaakt of ziet. 'Bloggen' is zo'n publiek dagboek online opstellen en de persoon die dit doet, noemen we een 'blogger'. Probeer het zelf eens!

TIP: "MIJN DIGITALE IK"

Zelf zo'n blog ineensteken kan op vele websites! Het is meestal gratis en heel makkelijk. Op http://spaces.live.com kan je zelfs je eigen achtergrond kiezen! In België bestaan al meer dan 1 miljoen Windows Live Spaces! Nu jij nog…

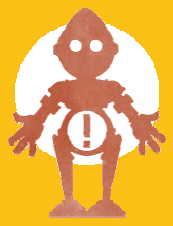
Waarom mag je je WEBLOG niet beschouwen als een gewoon DAGBOEK?



Een gewoon dagboek laat je niet zomaar door iedereen lezen. Je bewaart het op een speciale plaats en hangt er een slotje aan. Een blog kan door iedereen op internet gelezen en gezien worden! Vertel dus niet teveel persoonlijke dingen en kies geen privé-foto's om je blog te versieren. Je weet nooit wie je blog te zien krijgt en wat ze met deze informatie aanvangen…

TIP: "VIP ONLY!"

Wil je niet dat de hele wereld meekijkt naar je blog? Bij Windows Live Spaces kan je kiezen wie jouw geheimen mag lezen: iedereen, je Messenger contacten of enkele speciale vrienden uit je lijst. Kies in het menu voor 'Machtigingen'. Als je je blog beu bent, kan je de hele site verwijderen bij de 'Space-instellingen'.



Waarom moet je VOORZICHTIG? zijn met vrienden- of profielsites

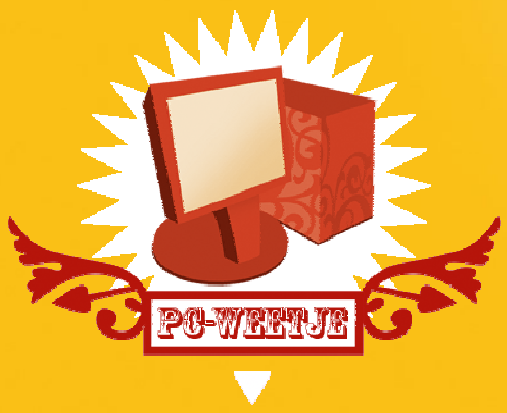
Er bestaan verschillende websites waar je zelf een pagina kan aanmaken en hiervoor je vrienden kan uitnodigen. Je verzamelt dan veel info over je vrienden en je kunt zelfs nieuwe vrienden maken. Plots heb je een heel 'netwerk' van kennissen! Best leuk, maar denk eraan dat ook onbekenden meer over jou te weten kunnen komen…Let dus op met persoonlijke gegevens in je profiel en toon niet je intiemste foto's.

Welke soorten BLOGS zijn er?

De meeste blogs zijn als een dagboek en gaan over dagelijkse gebeurtenissen. Daarnaast heb je ook meer serieuze blogs over zaken, politiek of nieuws. Veel surfers beweren zelfs dat sommige blogs sneller nieuws brengen dan de krant, radio of tv!

TIP: "ZEG HET MET EEN BLOG!"

Weet je niet wat je moet vertellen in je blog? Ideetjes vind je overal! Je hebt vast wel iets leuks beleefd op school, misschien heb je een leuke hobby of wil je later dokter worden? Zoek eens wat informatie op via een zoekrobot en je weet meteen weer iets bij! En zorg vooral dat je een blog maakt die je zelf graag zou bekijken.



Kan je ziek worden van te lang internetten?

Je wordt natuurlijk niet echt ziek van te internetten. Maar soms krijg je allerlei klachten als je te lang aan je computer zit. Je kunt hoofdpijn krijgen, pijn in je arm of schouder. Pijn in je arm door te veel te klikken op de muis noemt men zelfs een 'muisarm'. Neem dus op tijd een pauze, neem af en toe wat beweging en stop zeker als je ergens pijn hebt. Internet moet leuk blijven!

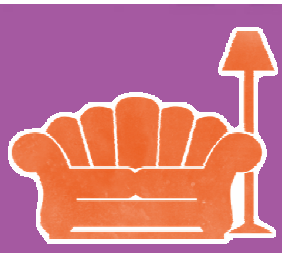
Wat is DOWNLOADEN?

Je hebt het zeker al gedaan: bestandjes binnenhalen op je computer. Liedjes, films, programma's of andere zaken haal je op tijdens het surfen op internet of het chatten in een babbelbox. Bij uploaden doe je net het omgekeerde van downloaden: je verstuurt een bestand van jouw computer naar een andere computer via het internet.

Mag je MUZIEK? *van het internet halen*

Ook op internet zijn er wetten, al lijkt het misschien alsof alles kan en mag. Je mag ook in het dagelijkse leven niet zomaar iemands werk gebruiken (liedjes, boeken, foto's, tekeningen, films...). Iedereen die iets maakt, mag daar geld voor vragen. Zomaar iets van internet halen zoals een film of liedje is net als een cd of dvd stelen in een winkel.

Mag je gratis gedownloade LIEDJES OF FILMS in je eigen kamer afspelen?

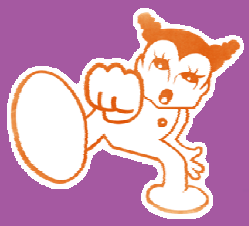


Neen, zelfs downloaden voor gebruik in je eigen huis is verboden. Je moet altijd de toestemming hebben van de maker of betalen. Steeds meer 'internetdieven' krijgen strenge straffen en boetes!

TIP: "MUZIEK VOOR NIETS!"

Af en toe kan je wel eens een gratis liedje meepikken als een artiest een nieuwe cd uitbrengt. Zo maakt de platenmaatschappij ook reclame voor dit nieuwe album!

Waar kan je downloaden zonder DE WET te overtreden?



Op bepaalde websites kan je voor een klein bedrag muziek en films downloaden. Die sites betalen een bijdrage aan de makers van het liedje of de film en je kunt er zeker van zijn dat de auteurs hun toestemming gegeven hebben aan de website om hun materiaal te gebruiken.

TIP: "LALALA-LAND!"

Leuke muziek kopen op internet kan o.a. op http://entertainment.msn.be/muziek. Je koopt vooraf een bepaald tegoed waarmee je kunt downloaden, net als beltegoed bij een gsm. Dit kan met een kredietkaart of sms. Het grote voordeel is dat je ook apart liedjes kan kopen in plaats van een hele cd in de winkel.

PC-WEETJE

Hoe kan ik online veilig betalen?

Als je iets online koopt, kan je dit met een kredietkaart betalen, per sms of via pc-banking (op de site van de bank). Net zoals in het echte leven zijn echter niet alle winkels even betrouwbaar. Vooraleer je kredietkaartinfo doorstuurt, check je best of de site wel veilig is en genoeg info geeft. Het adres van een beveiligde pagina begint meestal met de letters 'https' i.p.v. 'http'. Bovendien zie je vaak het beeld van een slotje onderaan je scherm of vermeldt de site simpelweg de naam van hun beveiligingssysteem. Informeer liefst je ouders ook vooraleer je iets bestelt.

Hoe beveilig ik best

MIJN PC?

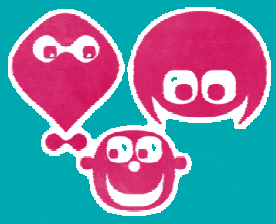
Met het besturingssysteem Windows Vista™maak je de veiligste keuze. Je beleeft nog meer plezier online, want surfen wordt betrouwbaarder! Je persoonlijke info op je pc wordt beschermd dankzij een vernieuwde Veilige Modus en verbeterde anti-phishing technologie. Bovendien blijft je computer ook tiptop presteren met de automatische spyware-scans van Windows Defender. Hiermee wordt schadelijke software dus echt verleden tijd!

TIP: "BLIJF UP-TO-DATE!"

Als Live Messenger-gebruiker kan je perfect op de hoogte blijven. Dankzij Live Security Alerts ontvang je de veiligheidsnieuwtjes heet van de naald! Schrijf je in op www.msn.be/alerts/microsoft!

Hoe zijn mijn ouders

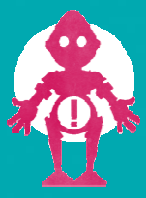
ZEKER *van mijn* VEILIGHEID? *op het internet*



Dankzij de nieuwe opties van Windows Vista™kunnen je ouders perfect toezien op jouw veiligheid. Voortaan kunnen ze sites met ongepaste inhoud blokkeren en eenvoudig bepalen welke spelletjes je mag spelen. Zo kunnen jullie samen ook je tijd op de computer beter in de hand houden. Je online plezier wordt er alleen maar beter op!

TIP: "WAAR VIND IK CONCRETE INFO OM MIJN PC TE BEVEILIGEN?"

De mogelijkheden om je PCte beveiligen worden steeds beter. Je kan de meest recente informatie om je Windows PCte beveiligen vinden op onze website: www.microsoft.be/athome/security. Hier ontdek je niet enkel hoe je jezelf kunt beschermen tijdens je online activiteiten, maar ook hoe je kunt voorkomen dat je persoonlijke gegevens in de verkeerde handen vallen.



Bibliografie

Boeken:

- VYNCKE, P., *Veilig op het internet – De complete gids voor veilig surfen*, Lannoo, Tielt, 2005, 496 pagina's
- DELVER, B., *Slim en safe internetten – Veilig internet voor en door kinderen*, Vives Media, Alkmaar, 2004, 126 pagina's
- Rymaszweski, M., JAMES AU, W., WALLACE, M., WINTERS, C., ONDREJKA, C., BATSTONE-CUNNINGHAM, B., ROSEDALE, P., *Second Life: het officiële handboek*, Omega, Diemen, 2007, 342 pagina's

Studies:

- VANDENBOSCH, H., VAN CLEEMPUT, K., MORTELMANS, D., WALRAVE, M., *Cyberpesten bij jongeren in Vlaanderen*, Studie in opdracht van het viWTA, Brussel, 2006, 211 pagina's

Websites:

- http://www.computerwoorden.nl
- http://www.wobotje.com
- http://www.computervirusalert.nl
- http://www.seniorennet.be
- http://www.wikipedia.org
- http://www.telenet.be
- http://www.dekinderconsument.nl
- http://www.iksurfveilig.nl
- http://www.clicksafe.be
- http://ond.vvkso-ict.com
- http://www.petervanvelthoven.be
- http://eid.belgium.be/
- http://www.surfopsafe.nl
- http://www.digibewust.nl
- http://www.peeceefobie.be
- http://www.ejustice.just.fgov.be
- http://www.internet-observatory.be
- http://www.polfed-fedpol.be
- http://www.ecops.be/webforms
- http://www.gva.be
- http://www.slpics.com

Onderwijs

RENO

KATHO

KATHOLIEKE HOGESCHOOL ZUID-WEST-VLAANDEREN
ASSOCIATIE K.U.LEUVEN

DEPARTEMENT LERARENOPLEIDING - RENO

departement lerarenopleiding RENO - campus Torhout - Sint-Jozefstraat 1 B-8820 TORHOUT

[t] 050 23 10 30 [f] 050 23 10 40 [e] reno@katho.be [w] www.katho.be/reno