

veilig  
internet

*Websites, gamen, chatten en e-mailen: het is natuurlijk vooral plezant, boeiend en praktisch. Toch moet je een beetje voorzichtig zijn. Je weet immers nooit zeker met wie je te maken hebt. Je kan het vergelijken met op straat lopen. Dat kan ook plezant zijn, maar wie oversteekt, moet goed uit z'n doppen kijken. Aan een kraampje op de markt betaal je niet voor een boek dat de marktkramer pas de volgende maand meebrengt. En als iemand op straat zomaar je rekeningnummer vraagt, dan is er toch geen haar op je hoofd dat er aan denkt om dit zomaar te geven.*

## E-mail

Elk e-mailbericht krijgt een stempel of 'header' en bevat zowel jouw adres als het adres van de zender. Krijg je een e-mailbericht met onbekend adres en de vraag om dit of dat te kopen, dan gaat het in principe om 'spam' of 'ongewenste e-mail'. Mensen met wie jij correspondeert, krijgen waarschijnlijk dezelfde rommel in hun bus.

Hoe e-mail je redelijk veilig?

- vermeld een duidelijk onderwerp, zodat de ontvanger je e-mail herkent als een 'serieus' bericht
- deel je e-mailadres alleen met mensen die je kent en vertrouwt
- gebruik spamfilters en virusscanners
- open spamberichten niet! Onderdruk je nieuwsgierigheid en reageer niet! Je krijgt alleen maar meer spam. Drop het meteen in de prullenmand!
- vraagt iemand om hem op te bellen, informeer dan eerst of het om een betaalnummer gaat en/of om een nummer in België. Stel je telefoon zo in dat niemand je nummer kan zien
- als een onbekende vraagt om een afspraak, ga er dan niet op in of vertel het aan je moeder of een vriend. De meeste mensen

hebben natuurlijk geen verkeerde bedoelingen, maar je weet nu eenmaal niks van die persoon. Alles wat je weet via het mailen, kan natuurlijk fake zijn. Bovendien, als hij cool of sympathiek is, dan is er ook niks op tegen dat je moeder weet waar je bent. Maar als hij uitzonderlijk toch een regelrechte griezels is, zal je blij zijn dat je vriend over een uurtje komt. Spreek die eerste keer in ieder geval af op een plaats waar andere mensen zijn of neem iemand mee. Zorg voor eigen vervoer. Dan kan je zelf beslissen wanneer je vertrekt. Wil die andere persoon dat niet, dan is er misschien reden om wantrouwig te zijn

## Chatten

Chatrooms voor 'instant messages' (MSN Messenger, ICO, AIM en Yahoo Instant Messenger) zijn fantastisch. Chatten met klasgenoten of gasten van het jeugdhuis, is natuurlijk oké. Maar achter nicknames van mensen die je niet kent, weet je nooit wie er schuil gaat. Wees dus liever voorzichtig.

Wat als iemand zich anders voordoet dan hij is? Zorg dat je daar niet op een pijnlijke manier en te laat achterkomt, b.v. door dat iemand tegen je zin alsmaar blijft bellen, je pest of chanteert, om niet te spreken van erger... Met MSN bepaal je zelf met wie je chat. Jij beslist wie er op je persoonlijke MSN-lijst komt te staan. Kopieer dus niet zomaar de MSN-adressen van je klasgenoten! Blokkeer onmiddellijk 'lastige' chatters.

### *Hoe chat je redelijk veilig?*

- laat je naam, voornaam, leeftijd, geslacht, adres, telefoonnummer en geheime codes niet achter op het net. Hou 'persoonlijke' gegevens 'persoonlijk'. Zelfs wanneer je chat met vrienden. Niet dat je hen moet wantrouwen, maar je weet nooit waar die informatie op die manier terecht komt. Voor je

# veilig internet

het weet, kan iedereen aan jouw gegevens. Anderen kunnen immers lezen wat je schrijft en dus ook gebruik maken van de informatie die jij op het web laat circuleren

- om in te schrijven in een chatroom moet je je profiel prijsgeven. Vul alleen die gegevens in die strikt noodzakelijk zijn of beperk je lijst van correspondenten tot mensen die je ook in het 'echte' leven kent
- hou in het menu 'tools/opties/berichten' van het e-mailprogramma bij met wie je chat
- stop als het vervelend wordt of als je je niet meer veilig voelt. Reageer nooit op pesten of schelden. Reageer nooit op iemand die je een ongemakkelijk gevoel geeft of van streek maakt. Praat er thuis over
- als een onbekende vraagt om een afspraak... zie onder ' E-mail'

## *Waar kan je terecht met een klacht?*

Je hoeft zeker niet alles te pikken! Meld vervelende chatters of situaties bij de moderator of beheerder van de chatroom. Bij MSN b.v. kan je contact opnemen met de abuse-afdeling. Ernstige klachten kan je aangeven bij de politie. Neem volgende gegevens mee: nickname en e-mailadres van de persoon die je lastigvalt, tijd en datum, naam of webadres van de chatroom en liefst een screenshot van de chatsessie (zie helppagina).

## **Surfen**

Surfen is een ideale manier om bekend te raken met het internet en informatie te vinden. Het springen van site naar site is plezierig en het kan een ware ontdekkingstocht worden! En toch is het niet helemaal onschuldig. Er kan spyware op je computer belanden, jouw privacy kan in het gedrang komen en je kan op sites met ongewenste of illegale inhoud terecht komen.

## Hoe surf je redelijk veilig?

- geef geen of zo weinig mogelijk persoonlijke gegevens prijs, ook niet in gastenboeken en op forums
- om ongewenste of illegale inhoud te vermijden kan een internet- of family-filter helpen (kan zeker via zoekmachines als Google en Alta Vista)
- installeer een anti-spywareprogramma en een firewall. Scan je computer regelmatig en zorg voor up dates
- gebruik een goede virusscanner
- installeer een popupkiller om het automatisch openen van (reclame-)schermen tegen te gaan
- verwijder regelmatig cookies van de computer. Een cookie is een klein bestand dat op je vaste schijf is geplaatst door een webpaginaserver. Een cookie onthoudt bepaalde instellingen, zoals taalkeuze. De volgende keer dat je naar die website surft, kom je automatisch terecht op de taal van jouw keuze
- verhoog de standaard veiligheidsinstellingen en privacyinstellingen van je browser en e-mailsoftware. Dit kan bijvoorbeeld bij de 'opties'

## Bestanden downloaden en doorsturen

Bestanden uitwisselen (tekst, muziek, video of beeld) is leuk of nuttig. Maar het kan ook gevaarlijk zijn want ze kunnen virussen bevatten. Virussen kunnen je computer definitief doen crashen! Je kan ook virussen krijgen van computers van bekenden! Dus: installeer een anti-virusprogramma en open bestanden nooit automatisch.

Een specifieke vorm om muziek, films en spelletjes uitwisselen, is P2P of 'peer to peer'. Er zijn talloze peer-to-peerprogramma's (b.v. Kazaa). Heel plezant, want het lijkt alsof je niet moet betalen. Maar

# veilig internet

dat lijkt alleen maar zo. Als je geen 'auteursrechten' betaalt aan de maker van de muziek, films of spelletjes, dan is verspreiding illegaal. Bovendien moet je er rekening mee houden dat je computer met P2P voor de andere 'peers' toegankelijk wordt, al weet jij niet wie dat zijn en wat die allemaal op je computer kunnen achterlaten. Als je b.v. een concert van je lievelingsgroep downloadt, kan je tegelijkertijd geweldadige en andere vunzige beelden ontvangen, die niets met dat concert te maken hebben. Maar ook gevaarlijke computervirussen kunnen zo op je computer belanden. Heb je bovendien geen firewall dan worden al jouw bestanden omgekeerd ook toegankelijk voor het hele P2P-netwerk. Dat betekent dat anderen toegang hebben tot jouw computer.

Heb je (naakt) geposeerd voor een webcam, dan kan jouw correspondent die foto's op het internet zetten. Dat kan heel vernederend zijn. Maar ook als je gewone vakantiefoto's doorstuurt, wil je wellicht niet dat de hele klas en zelfs de hele wereld tot in lengte van jaren die beelden kan bekijken. Maar zodra de beelden beginnen te circuleren, is er geen houden meer aan. Laat je dus niet forceren en dwing ook anderen niet. Stuur geen foto's of filmpjes door van vrienden zonder hun toestemming. Als ze akkoord gaan (je moet hun recht op privacy respecteren), is dit zeker niet illegaal op zich. Maar onthoud dat je nooit weet waar die filmpjes terechtkomen.

Omdat er geen tussenkomst is van een centrale server is opsporing op een peer-to-peerprogramma moeilijker. Juist daardoor heb je meer kans dat je vervelend, schokkend of strafbaar materiaal tegenkomt. Als je per ongeluk op mogelijk strafbaar materiaal stuit, verzamel dan informatie: naam van het programma, datum en tijd, gebruikersnaam, IP-adres, de zoekopdracht en de bestandnaam. Hieronder vind je plekken waar je terecht kan.

Krijg je foto's, filmpjes of teksten die je overstuur maken of kom je terecht op een website met een vulgaire, racistische, seksuele of andere inhoud waarvan je in de war raakt, stop dan onmiddellijk met chatten of surfen en breng de moderator van de chatroom, het forum of de website op de hoogte.

## **GSM**

Met een GSM kan je natuurlijk telefoneren. Maar je kan er ook mee SMS-en, gamen, chatten, surfen of e-mails ontvangen dankzij GPRS (General Packet Radio Service), foto's maken of video's opnemen met MMS (Multimedia Messaging Service) en die net zo makkelijk als een sms'je doorsturen.

Hou er rekening mee dat een GSM niet goedkoop is. Voor je bestanden of beltonen downloadt, informeer je best naar de prijs. Krijg je foto's die je onaangenaam of walgelijk vindt, reageer dan niet. Praat er over met anderen en/of laat het weten aan b.v. Child Focus of je mobiele operator.

### ***Hoe telefoneer je redelijk veilig?***

- denk na voordat je iemand je mobiele nummer geeft! Mobiele telefoons geven b.v. pestkoppen een nieuwe manier om mensen te pesten
- hou er rekening mee dat wat je doorstuurt, gebruikt kan worden op een manier die je niet wil of waar je je misschien voor schaamt

### ***Waar kan je terecht met een klacht?***

Doel melding via de site van je mobiele operator zodat die de pester kan zoeken en eventueel blokkeren. Pesten is niet strafbaar, maar als je echt zwaar gepest of gestalkt wordt, dan kan je naar de politie gaan. Neem het sms-bericht en het telefoonnummer mee van degene die je lastigvalt.

## Bloggen

Op het internet of via je GSM kan je makkelijk en (meestal) zonder kosten je dagboek publiceren. Op een blog kan je ideeën kwijt, vertellen over je hobby's, aankondigen welke fuif je aan het voorbereiden bent enz. Het is wel iets anders dan een intiem dagboek dat je op je kamer achter slot en grendel bewaart, want het kan gelezen worden door allerlei mensen, die je kent en die je helemaal niet kent.

### *Hoe blog je redelijk veilig?*

- hou er altijd rekening mee dat anderen dit ook lezen en er eventueel misbruik van kunnen maken (als bron voor plagerijen of door gegevens uit jouw blog te misbruiken)
- vermijd beschuldigingen en roddels over anderen, want ook dat kan weer door iedereen gelezen worden en veel leed veroorzaken

## Webcam

Via bepaalde webcams kan je op het internet bekijken hoe het weer is in Tokyo, Frankfurt, Los Angeles of Moskou. Met een webcam kan je ook videobeelden van jezelf maken én die op het internet zetten. Of je kan elkaar zien als je aan het chatten bent. Let op wat je doet voor een webcam b.v. tijdens het chatten. Je correspondent kan die beelden bijhouden en verspreiden over de hele wereld. Hou daar rekening mee! Er zijn helaas volwassenen (maar ook leeftijdsgenoten) die je willen verleiden om bepaalde dingen voor een webcam te doen. Zoals jezelf uitkleden. Van dit soort dingen kan je later spijt krijgen. Stel je voor dat iemand zo'n foto afprint en op het prikbord in de school hangt. Reageer niet op zo'n uitnodiging om naakt te poseren. Ook niet als je hiervoor geld krijgt. Als je filmpje straks voorgoed over de hele wereld verspreid raakt, krijg je misschien spijt, maar dan kan je de foto's niet meer terugkrijgen.

## Computer beveiligen

### *Virus*

Een virus is een programma dat gemaakt is om computers in de war te brengen of te beschadigen. Met een antivirusprogramma kan je virussen tegenhouden en je computer beschermen. Virussen verspreiden zich razendsnel over het internet. Ze verstopen zich vaak in een e-mail. Ook e-mail van je beste vriend kan dus een virus bevatten, zeker als hij vergeten is, zijn e-mailbox te scannen op virussen.

Installeer een virusscanner en hou die up-to-date. Er komen namelijk dagelijks nieuwe virussen bij. Stel je virusscanner zo in dat updates automatisch geïnstalleerd worden en dat hij alle schijven van je computer scant. Inclusief je e-mail!

### *Spyware*

Net als virussen nestelt spyware zich in je computer. Er wordt genoteerd welke websites je bezoekt, gegevens worden doorgestuurd en soms worden de instellingen van je browser aangepast. Zo kan je plotseling een andere startpagina hebben of verschijnen er websites waar je niet om gevraagd hebt!

Om je tegen spyware te beschermen, moet je regelmatig scannen met een antispywareprogramma. Er bestaan (gratis) programma's die spyware opsporen en verwijderen. Vergeet ook niet je antispywareprogramma up-to-date te houden!

### *Wet*

Over alle prettige, boeiende en praktische kanten van de media vind je in deze folder helemaal niks. Die ontdek je hopelijk zelf wel. Het werd een hele folder vol waarschuwingen. Er zijn aan deze media nu eenmaal bepaalde risico's verbonden. Er zijn ook wetten die proberen die risico's zoveel mogelijk te verkleinen.

Zo zijn er wetten tegen het verboden gebruik van informatie. Je kan foto's, liedjes, films enz. allemaal bekijken, maar je mag ze je niet toe-eigenen. Er staat immers een 'auteursrecht' op. Het blijft m.a.w. eigendom van wie het gemaakt heeft. Je mag dat materiaal niet zomaar kopiëren en doen alsof jij het hebt gemaakt. Zie 'Auteursrecht'.

Daarnaast is er de wet ter bescherming van de privacy: je hoeft nooit je naam, leeftijd of adres te geven. Doe je dat toch, dan zegt de wet dat je altijd mag kijken welke informatie men over jou bewaart. Je mag die gegevens ook corrigeren. De persoon aan wie jij die gegevens 'geeft', mag die zonder jouw toestemming niet aan anderen doorgeven.

Er is ook een wet tegen computercrackers. Een cracker kan proberen je wachtwoord en het nummer van je kredietkaart te ontcijferen. Hij kan dan op jouw kosten allerlei aankopen doen via het internet. Natuurlijk is dat strafbaar. Maar het is moeilijk toe te passen. Als er in een huis wordt ingebroken, dan kan je de politie bellen. Zij gaan dan op zoek naar sporen die kunnen vertellen wie de inbreker is. Maar iemand die in een computer inbreekt, kan ook aan de andere kant van de wereld wonen. Daarom zijn er internationale afspraken om computercriminaliteit te bestraffen. Maar door de wereldwijde schaal van het internet is het natuurlijk heel wat moeilijker op het effectief toe te passen.

## Adressen, folders en websites

### *Informatie en meldpunt*

Op [www.clicksafe.be](http://www.clicksafe.be) vind je informatie over de risico's van surfen en chatten en tips om problemen te vermijden. Als je iets gekks of eigenaardigs tegenkomt waarover je je zorgen maakt, dan kan je dat melden via [clicksafe@childfocus.org](mailto:clicksafe@childfocus.org). Je kan ook contact opnemen met de federale politie via [contact@fccu.be](mailto:contact@fccu.be).

# veilig internet

[www.web4me.be](http://www.web4me.be) is een website voor een veiliger internet, gecoördineerd door verbruikersorganisaties OIVO (02/547.06.11). Hier vind je informatie over problemen die je kan tegenkomen op het internet: consumentenbescherming, sekten, misbruik van foto's, een virusaanval, louche teksten, beledigingen, een bug in je PC enz. Op deze site vertelt men hoe je kan reageren en wat je kan doen om die problemen in de toekomst te vermijden.

Andere klachten kan je melden bij de abusedesk van de service-dienst die je gebruikt. Bij MSN is dat <http://groups.msn.com/feedback.msn>

Lijkt er iets mis met je zoekopdracht, neem dan contact op met de Zoekmachine.

Bij Google is dat: [www.google.nl/intl/nl/webmasters/spamreport.html](http://www.google.nl/intl/nl/webmasters/spamreport.html).

Op [www.onderzoekjegrens.nl](http://www.onderzoekjegrens.nl) kan je een test doen om er achter te komen waar jouw grenzen liggen op het gebied van privacy, intimiteit en seksualiteit.

## **Spam**

Spam, verstuurd vanuit België, kan je melden via [abusespam@isoc.be](mailto:abusespam@isoc.be). Je kan alleen een klacht indienen over spam die verzonden is aan een e-mailadres dat bij een persoon in gebruik is (dus geen info@, sales@,...), die een bedreigend of commercieel karakter heeft en waarvan de verzender (degene die op de verzendknop drukt of degene die opdracht geeft tot de verzending) zich in België bevindt.

Spam, verstuurd vanuit het buitenland, kan je melden bij de e-mailprovider van de spammer. In de header van het e-mailbericht kan je het IP-adres vinden vanwaar de spam is verstuurd. Er zijn diverse antispamsites waar je dit kan melden.

## **Ongeoorloofde informatie op het internet**

Ongeoorloofd veronderstelde informatie (b.v. kinderpornografie, racisme, kansspelen) kan je aangeven via [contact@gpj.be](http://contact@gpj.be).

Informaticacriminaliteit beperkt zich niet tot specifieke misdrijven zoals b.v. hacking, waarbij de computers zelf centraal staan. Het kan ook een middel zijn om andere misdrijven te plegen. Inbreuken begaan via het internet kunnen op grond van het strafwetboek en bijzondere strafwetten bestraft worden.

### ***Auteursrecht***

'Auteursrecht en internet' van prof. Mireille Buelens kan je gratis bestellen bij de Federale diensten voor wetenschappelijke, technische en culturele aangelegenheden op het nummer 02/238.35.19 of via [vdpu@belspo.be](mailto:vdpu@belspo.be). Je kan het dossier ook raadplegen via [www.belspo.be/belspo/home/publi/pub\\_ostc:d\\_auteur/tm1nl.pdf](http://www.belspo.be/belspo/home/publi/pub_ostc:d_auteur/tm1nl.pdf).

'Auteursrechtgids voor Nederland en België' van Frequin en Vanhees, een basisboek met informatie voor juridische leken (288 blz.) is uitgegeven door Standaard uitgeverij. Bestellen kan via 03/285.72.00 of via [algem@standaard.com](mailto:algem@standaard.com).

### ***Kinderporno***

De verspreiding van kinderporno via een computernetwerk is strafbaar. Ook het bezit op harde schijf, diskette of enig ander elektronisch of optisch medium valt onder de bepalingen van deze wet. Aangifte kan via [www.gpj.be/nl/meld\\_kp.htm](http://www.gpj.be/nl/meld_kp.htm). Sites met kinderporno kan je ook melden via [www.childfocus-net-alert.be](http://www.childfocus-net-alert.be).

### ***Discriminatie en Racisme***

Beledigingen en propaganda voor racisme en discriminatie kan je melden via [www.cyberhate.be](http://www.cyberhate.be).

### ***Geschokt? Gepest?***

Word je gepest, dan kan je gratis bellen met de Kinder- en Jongerentelefoon op nummer 102. Je kan er je verhaal kwijt en de medewerker zal proberen je te steunen. Meer info over pesten vind je op [www.pestening.nl](http://www.pestening.nl), [www.laks.nl](http://www.laks.nl), [www.pestweb.nl](http://www.pestweb.nl) of [www.pestenislaf.nl](http://www.pestenislaf.nl).

# JIP

## En dan is er ook nog het JIP!

Wil je meer uitleg over dit thema? Wil je één van de vermelde websites of folders bekijken? Loop dan binnen in het JIP of jongereninformatiepunt. Je kan er terecht met vragen of problemen in verband met wonen, werk, seks, relaties, sport, jeugdverenigingen, vorming, drugs, geld, cultuur, toerisme, mobiliteit, gezondheid, onderwijs, geweld enz.

In een JIP kan je zelf informatie opzoeken, maar je bent er ook welkom voor een gesprek. Als je wil, zoekt de JIP-medewerker mee naar een antwoord op je vraag of een oplossing voor jouw probleem. Heb je verder advies, hulp of begeleiding nodig, dan word je doorverwezen naar een persoon of dienst die je verder kan helpen.

Voor het adres en het telefoonnummer van een JIP in de buurt: zie [www.jips.be](http://www.jips.be).



Najaar 2006



Delta vzw - Netwerk van JIPS  
Vijverlaan 53 • 2610 Wilrijk • T. 03/820.95.31 • [info@jips.be](mailto:info@jips.be)  
[www.jips.be](http://www.jips.be)