

# Handleiding voor ouders

Leer uw kinderen veilig internetten





# INHOUD

## A. Hoe gebruikt u dit pakket?

p. 4



## B. Handleiding voor ouders en opvoeders

p. 5



### 1. Beveiligd en wel

p. 6

### 2. Communiceren LoL ;-D

p. 10

### 3. Cyberpesten

p. 15

### 4. Entertainment & Downloaden

p. 17

## C. Voorgestelde oplossingen bij de activiteiten

p. 21



### 1. Beveiligd en wel

p. 21

### 2. 2. Communiceren LoL ;-D

p. 24

### 3. Cyberpesten

p. 26

### 4. Entertainment & Downloaden

p. 27

## D. Glossarium

p. 29



## E. Nuttige adressen

p. 39





## A. Hoe gebruikt u dit pakket?

***Als je een jaar vooruit plant, plant dan rijst.***

***Als je tien jaar vooruit plant, plant dan een boom.***

***Als je een leven lang vooruit plant, onderwijs dan je kind***

*Chinees gezegde*

Beste ouder,

Het internet mag geen kloof slaan tussen de generaties, maar moet hen net samenbrengen, Daarom hebben we dit Veilig Internet Gezinspakket voor u ontwikkeld. Het pakket is bedoeld voor gezinnen met kinderen tussen 6 en 12 jaar. Het is samengesteld door Insafe, een Europees netwerk dat de verschillende, door de Europese Commissie gefinancierde, initiatieven rond veilig internet, die plaatsvinden in alle Europese lidstaten, ondersteunt. Saferinternet.be is de naam van het Belgische project. Alle verdere info vindt op de gelijknamige site. Dit Gezinspakket kwam in ons land tot stand met de steun van Telenet.

Spelen in de speeltuin of op straat kan gevaarlijk zijn als je niet oplet en/of de regels niet kent. Dat is ook zo als je het internet of mobiele technologieën gebruikt. Je moet dus voorzichtig zijn. En er op een slimme en veilige manier mee (leren) omspringen.

Gebruik dit nieuwe pakket om uw kinderen te leren om veilig en efficiënt gebruik te maken



van het internet. Het bevat ruim vijftig veiligheidstips en oefeningen waarmee uw kinderen op een leuke, plezierige en niet-bedreigende manier kunnen kennismaken met een veilig internet. Het pakket bestaat uit:

- Twee boekjes over veiligheid op het internet: een familie-fun-boekje en een handleiding voor ouders;
- Praktische tips (de zogenaamde “hoofdregels”);
- Een gezinscertificaat;
- Een stickerset;
- 12 kaartjes met verschillende situaties die de kinderen kunnen uitknippen.

Zowel het familie- als het ouderboekje zijn voorzien van kleurencodes. Die gebruiken we om vier belangrijke aspecten van veilig internet toe te lichten: **Beveiliging**, **Communiceren**, **Entertainment & Downloaden** en **Cyberpesten**. Het ouderboekje dient als naslagwerk voor het familie-fun-boekje: het bevat achtergrondinformatie, opmerkingen bij de activiteiten en oplossingen voor de oefeningen en de situatiekaartjes. Het familie-fun-boekje moet door de kinderen en de ouders samen gebruikt worden.

De vier thema's worden besproken aan de hand van een verhaal over twee kinderen, Alex en Emma, hun ouders en de IT-expert Laura. Elk hoofdstuk bevat leerzame activiteiten, zoals online oefeningen, toetsjes, praktische regels en handige links.

Lees het verhaal samen met uw kinderen en werk samen aan de voorgestelde activiteiten. Aan het einde van elk hoofdstuk kunt u de bijbehorende situatiekaartjes gebruiken om een gesprek met uw kinderen te starten en zo hun begrip van de inhoud verder te verdiepen.

Als uw kinderen enthousiast met het pakket aan de slag gegaan zijn, kunt u ze belonen door met z'n allen het gezinscertificaat te ondertekenen en een aantal hoofdregels af te spreken. Tot slot kunnen uw kinderen de boekjes nog versieren met de emoticonstickers.

Aarzel niet om contact op te nemen met ons als u vragen of opmerkingen heeft. Uw commentaar is waardevol voor ons.

We wensen u en uw gezin veel plezier op het internet! En veel veilige surftochten!

Insafe en Saferinternet.be



Dit pakket kwam tot stand met de steun van Telenet.



## B. Handleiding voor ouders en opvoeders

# 1. Beveiligd en wel



## EEN COMPUTER IN HUIS HALEN

Een computer in huis kan heel leerzaam en ontspannend zijn voor het hele gezin. Door de computer in een gezamenlijke ruimte te zetten en goede afspraken te maken met uw kinderen, houdt u het veilig voor hen.

Vergeet niet dat uw kinderen ook op het **internet** kunnen bij vriendjes en vriendinnetjes, in internetcafés etc. Het is daarom van belang om samen met hen veilige en goede gedragsregels op te stellen die ze altijd en overal kunnen toepassen.

## UW COMPUTER BEVEILIGEN

Als je een veilige omgeving kan wil creëren, moet je oplossingen bedenken voor de potentiële risico's. Zo kan het installeren van nuttige technologische hulpmiddelen een deel van

de oplossing zijn. Maar ook met gezond verstand kom je al een heel eind verder.

Het gebruik van **geheugensticks** of **cd-roms**, het openen van **bijlagen** en downloaden van bestanden kan gevaarlijk zijn. Ze kunnen namelijk kwaadaardige **computerprogramma's (malware)** bevatten, die zijn ontworpen om uw computer schade toe te brengen, persoonlijke gegevens te stelen of ongevraagd reclame rond te sturen.

Kinderen maken in het familie-fun-boekje kennis met diverse soorten malware, zoals **virussen**, **wormen**, **Trojaanse paarden** en **spyware** en leren de symptomen van een geïnfecteerde computer herkennen. Ze leren hoe ze besmetting kunnen voorkomen door alleen te internetten op een computer die is beschermd door **antivirus-** en **antispywareprogramma's** die up-to-date zijn. Er wordt hen ook aangeraden om voorzichtig te zijn als ze e-mailbijlagen van onbekende afzenders openen, programma's van het internet downloaden en USB-sticks of cd-roms gebruiken.

## SPAM BESTRIJDEN

80% van alle e-mails die op het internet circuleren, is **spam** (ongewenste e-mail). Ook uw kinderen komen hiermee in aanraking. Wie zonder opletten en nadenken zijn **e-mailadres** op het **web** publiceert, bijvoorbeeld in een **nieuwsgroep**, **chatsite**, een openbaar **forum**, een **social networkingsite** of een **online formulier**, zal meer te maken krijgen met spam. Er bestaat immers software die het internet afschuimt, op zoek naar e-mailadressen om zo adreslijsten samen te stellen die vervolgens worden gebruikt om in enorme hoeveelheden spam te verspreiden. De bedrijven die zich met dergelijke activiteiten bezighouden, zijn vaak gevestigd op plaatsen waar geen wetgeving bestaat omtrent ongevraagde e-mail.

Meestal wordt spam verspreid met frauduleuze bedoelingen. Vaak gaat het bij spam over het aanbieden van pornografie, medicijnen, dubieuze financiële transacties etc. Bovendien kan spam ook een bron zijn van kwaadaardige programma's. Hieronder volgen enkele tips om uw gezin te beschermen:

- Gebruik "**spamfilters**". Uw e-mailprovider biedt doorgaans antispamfuncties aan die u in uw e-mailprogramma kunt activeren. Vraag hem om meer informatie. Controleer ook regelmatig of er in uw **junkmail-** of **spammap** geen onschuldige e-mails zijn beland. Technologie is immers niet onfeilbaar.
- Leer uw kinderen om e-mail van onbekenden niet te openen. Spam ziet er bijna altijd uit als uitnodigende aanbiedingen en bijlagen. Laat ze zien hoe je de afzender van een e-mail moet blokkeren en leer hen om verdachte e-mails gewoon te verwijderen.

## SURFEN OP HET NET

Ook voor heel jonge kinderen is het nuttig en leuk om op het internet te surfen en leerzame **websites** te bezoeken. Maar het internet bevat ook zaken die niet geschikt zijn voor jonge surfertjes. Zoekmachines zijn ideaal om informatie op te zoeken op het internet. Maar omdat het zoeken afhankelijk is van de gekozen zoektermen, kun je ook snel ongewenste inhoud tegenkomen. Een onschuldig klinkende zoekterm kan een niet zo onschuldige website opleveren die de zoekterm in kwestie

bevat. Hieronder volgen enkele tips om uw kinderen veiliger te laten surfen op het internet:

- Maak met een **besturingssysteem** (bijv. Windows, Linux, Mac OS) een speciale gebruikersaccount voor uw kind waarop u een functie voor **ouderlijk toezicht** kunt activeren;
- Ga ook de functies voor ouderlijk toezicht op uw **internetbrowser** en zoekmachine na. Weet dat u ook hier de **gezinsinstellingen** kan aanpassen.
- Stel jonge kinderen een kindvriendelijke **zoekmachines** in.
- Sla de adressen van de websites die uw kinderen het meest gebruiken op in hun map **Favorieten** (een browserfunctie). Zo kunnen ze steeds weer naar hun favoriete sites op het **net** surfen zonder een zoekmachine te moeten gebruiken.

Naast het activeren van de functies voor ouderlijk toezicht op uw browser en zoekmachine, kunt u nog een aanvullende **filter** gebruiken. Een filter is software die gemaakt is om minderjarigen te beschermen tegen inhoud op het web die niet voor hun ogen bestemd is. Win advies in bij uw internetaanbieder of zoek op het internet naar **proefsoftware**. Maar vergeet niet dat niets de begeleiding van ouders en opvoeders kan vervangen. Technische hulpmiddelen zijn immers niet onfeilbaar en kunnen soms een vals gevoel van veiligheid geven, tenzij ze gebruikt worden in combinatie met gezond verstand, opvoeding en communicatie.

Bovendien kunnen filters zodanig beperkend werken dat ze onschuldige inhoud blokkeren. Kinderen kunnen dan bijvoorbeeld geen informatie over de Tweede Wereldoorlog opzoeken voor een geschiedenis huiswerk, omdat die zoektocht leidt naar websites waarop geweld beschreven wordt. Bovendien kan een geactiveerde filter ook weer worden gedeactiveerd door slimme jongeren die meester zijn in het uitwissen van hun sporen. Het is dan ook essentieel dat u ook zelf leert hoe u de computer en de software moet gebruiken.

Bezoek de website van **SIP-Bench** ([www.sip-bench.eu](http://www.sip-bench.eu)). In deze door de Europese Commissie gesteunde studie, werden 30 hulpmiddelen voor ouderlijk toezicht en antisphulpmiddelen getest op hun doeltreffendheid om kinderen tussen 6 en 16 jaar te beschermen tegen schadelijke inhoud van diverse internettoepassingen: **browsen**, e-mailen, **bestanden versturen**, chatten en **instant messaging**.

Naast het vermijden van **schadelijke inhoud** moet u ervoor zorgen dat uw kinderen niet alles geloven wat ze zien of lezen op het internet. In het familie-fun-boekje raden we hen aan bij het zoeken naar informatie altijd minstens 3 websites te bekijken en de inhoud ervan te vergelijken. Ze krijgen ook het advies om voor een schoolopdracht altijd de bron van de gevonden informatie te vermelden.

## HOOFDREGELS VOOR OUDERS VAN SURFENDE KINDEREN

- Zorg dat uw computer is beveiligd met een **firewall**, antivirus- en antispywaresoftware. Houd deze up-to-date en let op eventuele **alarmsignalen** die ze geven. Controleer of uw internetaanbieder antivirus- en antispywarehulpmiddelen aanbiedt die u kunt gebruiken;
- Gebruik een spamfilter op uw e-mailprogramma en houd uw e-mailadres zoveel mogelijk voor uzelf door het niet op het web te publiceren. Mijd e-mails van onbekende afzenders en **scan** bijlagen voordat u ze opent;



- Benut zoveel mogelijk de functies voor ouderlijk toezicht van uw besturingssysteem, internetbrowser, zoekmachine en e-mailprogramma. Maak aparte **gebruikersaccounts** voor uw kinderen. Stel privacyinstellingen zo hoog mogelijk in (ga naar het menu "Extra" in uw browser);
- Overweeg om voor jonge kinderen aanvullende filtersoftware te gebruiken;
- Neem direct contact op met uw internetaanbieder of een expert als uw computer zich vreemd gedraagt. Uw computer kan immers geïnfecteerd zijn;
- Als u kinderpornografische beelden op het internet ontdekt, meld dit dan via [www.stopchildporno.be](http://www.stopchildporno.be). Racistische of discriminerende inhoud kan u melden via [www.cyberhate.be](http://www.cyberhate.be);
- Ga eens naast uw kinderen zitten als ze aan het surfen zijn. Dit is een uitstekende manier om het gesprek te starten en het vertrouwen te vergroten. Maak er een uitdaging van om samen te leren;
- Onthoud dat deze veiligheidsregels zowel op u als op uw kinderen van toepassing zijn. Moedig hen aan het u te vertellen als ze vreemde dingen tegenkomen.

## HANDIGE LINKS

Om veilig te kunnen surfen, is kennis essentieel: weten wat de risico's zijn, weten hoe u zichzelf kunt beschermen en nog meer kennis kan opdoen. Veel meer informatie vindt u op de website [www.saferinternet.be](http://www.saferinternet.be)

Actuele informatie, tips en links over veilig internetten voor ouders, leerkrachten, kinderen en jongeren is te vinden op [www.clicksafe.be](http://www.clicksafe.be)

[www.gezinsbond.be/veiligonline](http://www.gezinsbond.be/veiligonline) legt ouders klaar en duidelijk uit wat de voordelen en de risico's zijn van de nieuwe technologieën en geeft heel wat tips over hoe deze thematiek in de opvoeding kunnen geïntegreerd worden. De technische kant van de zaak wordt uitgelegd via demofilmpjes.

Voor leerkrachten werd door het Vlaams Departement Onderwijs de brochure 'Veilig online. Tips voor veilig ICT-gebruik op school' ontwikkeld, in samenwerking met o.a. het OIVO en Child Focus. Deze brochure heeft ook veel aandacht voor veilige wachtwoorden, firewalls, virussen, spam, computerbeveiliging enzovoort. Zie <http://www.ond.vlaanderen.be/ict/ondersteuning/veiligICT>. Bij de brochure hoort ook een cd-rom met digitale lespakketten.

Surf eens naar [www.spamsquad.be](http://www.spamsquad.be), de Belgische portaalsite in de strijd tegen spam.

De laatste resultaten van de SIP Benchmarkstudie vindt u op [www.sip-bench.eu](http://www.sip-bench.eu)

Als u kinderpornografische beelden op het internet ontdekt, meld dit dan via [www.stopchildporno.be](http://www.stopchildporno.be). Racistische of discriminerende inhoud kan u melden via [www.cyberhate.be](http://www.cyberhate.be);  
Een algemeen overheidsmeldpunt voor internetmisbruik in België is [www.ecops.be](http://www.ecops.be)

## 2. Communiceren LoL ;-D



### PUZZELSTUKJES

Weet u nog hoe belangrijk u het vroeger vond om contact te houden met uw vriendjes en vriendinnetjes? Op het internet zijn veel nieuwe plaatsen om vrienden te ontmoeten en nieuwe manieren om met elkaar te communiceren: e-mailen, **bestanden delen**, **bloggen** en social networking (bijv. Netlog, MySpace, Facebook, Habbohotel) etc. Tieners gebruiken tegenwoordig informatie- en communicatietechnologieën (ICT) om nieuwe dingen uit te proberen en elkaar te ontmoeten in een omgeving die zij beschouwen als persoonlijk en vrij van ouderlijk toezicht.

Het hoofdstuk over communiceren in het familie-fun-boekje laat ouders en kinderen kennismaken met begrippen als **persoonlijke gegevens**, **privacy**, positieve online interactie en het omgaan met risico's, zoals contact met vreemden.

Online privacy hangt nauw samen met **accounts & profielen**. Een account hebt u nodig om toegang te krijgen tot een online dienst. In de echte, offline wereld bevat een busabonnement of een lidmaatschapskaart persoonlijke informatie over de houder ervan. Online accounts en diensten zijn daarmee te vergelijken. U kunt er geen gebruik van maken zonder enkele persoonlijke gegevens door te geven die worden gebruikt om uw "gebruikersprofiel" op te stellen. Het is van belang dat u zelf kunt bepalen welke informatie u over uzelf ter beschikking stelt en met wie u deze informatie wilt delen.

Als u uw privacy wil beschermen, moet u uw persoonlijke informatie beheren. Liegen is daarvoor niet nodig, denk gewoon goed na voor u uw gegevens ergens invult. Jongeren zijn vaak enthousiast over hun online communicatie met vrienden en hun online imago. Ze staan echter niet altijd stil bij de gevolgen van het openbaar maken van persoonlijke informatie.

### EEN PROFIEL AANMAKEN

De eerste stap in het beschermen van persoonlijke informatie is de aanmaak van een veilig profiel door zorgvuldig na te denken over de gegevens die erin zullen worden opgenomen en de privacy-instellingen die u wilt toepassen.

Maak aparte e-mailaccounts aan voor verschillende online contexten. Moedig uw kind aan een neutraal e-mailadres en een neutrale nickname te gebruiken bij het chatten, instant messaging, bloggen etc. Zo gebruikt uw kind geen e-mailadres waarmee zijn/haar volledige naam bekend wordt.

Houd **wachtwoorden** van accounts altijd geheim. Zorg ervoor dat uw kinderen begrijpen dat ze dit niet moeten delen met anderen die later mogelijk misbruik kunnen maken van hun vertrouwen.

Vergeet niet de **privacyinstellingen** van uw profiel/account aan te passen van openbaar naar persoonlijk. Zo hebt u zelf in de hand voor wie uw gegevens zichtbaar zijn en met wie u contact kunt hebben. Met een persoonlijk profiel kunt u immers bepalen wie er op uw **contactpersonenlijst** komt te staan. Leer uw kinderen om alleen contactpersonen toe te voegen die ze offline ook kennen.

Als uw kinderen gebruikmaken van chatrooms ga dan na of:

- er echte **moderators** aanwezig zijn. Geen moderator betekent dat er niet veilig kan worden gechat;
- er functies zijn waarmee ongewenste chatters kunnen worden genegeerd of geblokkeerd;
- er een help- en **rapporteringsfunctie** op de website is waar ze gebruik van kunnen maken als er problemen zijn;
- de regels van de dienst duidelijk en zichtbaar vermeld zijn.

## FOTO'S EN WEBCAMS

Kinderen moeten begrijpen dat hun foto een wezenlijk deel uitmaakt van hun privacy en dat digitale afbeeldingen zeer krachtig en invloedrijk zijn. Ze kunnen gemakkelijk verspreid en **bewerkt worden** en kunnen zeer moeilijk gewist worden wanneer ze eenmaal via een computer of mobiele telefoon zijn verstuurd. Zo kunnen ze heel lang online blijven staan! U en uw kinderen zouden persoonlijke afbeeldingen alleen mogen delen met mensen die u kent en vertrouwt. Vraag ook altijd toestemming voordat u een foto van iemand anders publiceert. **Webcams** moeten met de nodige voorzichtigheid worden gebruikt en jonge kinderen gebruiken de webcam best niet zonder toezicht. Laat uw kinderen dus geen computer en webcam gebruiken als ze alleen op hun kamer zijn.

## CONTACT MET VREEMDEN

Mensen die u online ontmoet, zijn niet altijd wie ze beweren te zijn. Leer uw kinderen om hun privacy online te beschermen, net zoals ze dat in de echte, offline wereld zouden doen. U maakt met hen afspraken over hoe ze in de echte wereld met vreemden moeten omgaan, dus waarom zouden ze zich op het internet niet aan diezelfde afspraken moeten houden?

Kinderen bouwen soms intense vriendschappen op met online vrienden. In het algemeen hebben kinderen de neiging om mensen die belangstelling voor hen hebben, die met hen praten en naar hen luisteren, veel te makkelijk te vertrouwen, zelfs als ze deze mensen niet zo goed kennen. Na vijf minuten chatten beschouwen ze die persoon vaak al als een vriend. Daardoor kan de verleiding groot zijn om in het echt met deze nieuwe vrienden af te spreken zonder dat ze u hierover inlichten. Kinderen zijn zich vaak niet bewust van het potentiële gevaar van zulke afspraken. Praat hierover met uw kinderen. Leer hen om, als ze dan toch een afspraak maken, steeds af te spreken op een openbare plaats en om een vertrouwenspersoon mee te nemen. Communiceren is essentieel !!

## NETTIQUETTE

**Netiquette** staat voor goede manieren op het internet. Het betekent eigenlijk dat je mensen online behandelt zoals je zelf ook graag behandeld wil worden. Kinderen beseffen soms niet dat zij online iemand kunnen beledigen, zonder dat dat hun bedoeling was. De ander ziet je lichaamstaal namelijk niet. Helaas gebruiken sommige mensen het internet en/of de gsm om anderen boos of verdrietig te maken of te pesten. Dit wordt cyberpesten genoemd, een probleem waar veel kinderen mee te maken krijgen (zie het hoofdstuk Cyberpesten voor meer informatie).

## CHATTAAAL

Als jongeren online chatten, gebruiken ze een unieke taal vol **emoticons** en **acroniemen!** Bekijk onderstaande tabellen om er bekend mee te raken 😊

Indicatieve lijst van chatacroniemen:

121: one to one	JJ: just joking
AFK: away from keyboard	K: all right /ok
A/S/L: age, sex, location (or just „ASL“)	KFY/K4Y: kiss for you
BBB: bye bye baby	KISS: keep it simple, stupid
B4N: bye for now	KPC: keeping parents clueless
BBL: be back later	L8R: later
BF: boyfriend or best friend	IRL: in real life
BFF: best friends forever	LMIRL: let's meet in real life
C: see?	LOL: laughing out loud, lots of love
Comp: computer	LY4E: love you forever
CU: see you	NE1: anyone
CUL: see you later	NP: no problem/ noisy parents
CYO: see you online	OIC: oh, I see
EGBOK: everything going to be ok	OLL: online love
F2F: face to face	PAL: parents are listening
G2G or GTG: got to go	PAW: parents are watching

<G>: grin

GF: girlfriend

GFN: gone for now

GL: good luck

GM: good morning /good match

HAND: have a nice day

^5: High 5

H2G: have to go

HDOP: help delete online predators

IDK: I don't know

ILU/ILY: I love you / I like you

PIR: parent in room / people in room

PLZ/PLS: please

POS: parent over shoulder

RL: real life

S^, S'UP: what's up?

TTYL: talk to you later

TY: thank you

WB: welcome back/ write back

WDYT: what do you think

WTGP: want to go private?

WYCM: will you call me?

Emoticons maakt u door leestekens en letters te combineren:

Smiley (met of zonder neus)

:) or :-)  
dubbelpunt, (streepje), haakje

Verdrietig gezichtje  
(met of zonder neus)

:( or :-(  
dubbelpunt, (streepje), haakje

Knipogend gezichtje (met of zonder neus)

;) or ;-)  
puntkomma, streepje, haakje

Verbaasd gezichtje (met of zonder neus)

:o or :-o  
dubbelpunt, (streepje), kleine o

Brede lach (met of zonder neus)

:-D or :D  
dubbelpunt, (streepje), hoofdletter D

Tong uitsteken (met of zonder neus)

:p or :-p  
dubbelpunt, kleine p

## HOOFDREGELS

- Neem de tijd om te ontdekken hoe uw kinderen hun tijd online doorbrengen en vraag hen om u te laten zien hoe ze met hun vrienden communiceren;
- Leer ze om hun privacy online te beschermen door:
  - Veilige profielen aan te maken met ingeschakelde privacy-instellingen, altijd een nickname te gebruiken als ze chatten en onbekende mensen te verwijderen uit hun chat-contactlijst.
  - Hun wachtwoorden te beschermen
  - Alleen contact te leggen met en berichten te beantwoorden van mensen die ze ook offline kennen
  - Altijd uw toestemming te vragen voordat ze foto's van zichzelf, uw gezin, huis, hun school etc. uploaden
  - Persoonlijke informatie, zoals hun naam, e-mailadres, telefoonnummer, adres, school, sportteam etc., nooit online aan iemand toe te vertrouwen, tenzij ze die persoon ook in het echt goed kennen. Op websites, social networkingsites of in communicatie met vreemden is het volledig uit den boze om persoonlijke informatie prijs te geven.
- Zet de computer in een gezamenlijke ruimte zodat u toezicht kunt houden op hun online activiteiten;
- Zorg er samen voor dat u:
  - Weet hoe u contactpersonen kunt weigeren of personen kunt blokkeren in een contactpersonenlijst
  - Op de hoogte bent van de veiligheids- en rapporteringsfuncties die beschikbaar zijn op de door u gebruikte websites
- Bouw vertrouwen op door uw kinderen ervan te verzekeren dat ze met u ook kunnen praten over hun fouten, zodat u samen naar een oplossing kunt zoeken! Fouten maken hoort bij het leerproces.

## HANDIGE LINKS

Op [www.saferinternet.be](http://www.saferinternet.be) vind je meer info over veilig en slim communiceren en privacy online. Zie o.a. de 'Tips voor cyberkids' en het spelletje Spotm'nblog. Het spel heeft veel aandacht voor het gebruik van persoonlijke contactgegevens online, een nickname kiezen, foto's gebruiken, ... Bij het spel hoort ook een handig pedagogisch dossier voor leerkrachten en ouders.

Op [www.e-privacy.be](http://www.e-privacy.be) vind je meer info over jongeren en privacy online, o.a. de studie 'Cyberkids' e-Privacy' waaruit bleek dat een meerderheid van de websites die bestemd zijn voor kinderen en jongeren persoonsgegevens van deze jonge bezoekers verzamelt zonder hun privacyrechten te respecteren.

[www.clicksafe.be](http://www.clicksafe.be) geeft ook heel wat nuttige tips mee.

Op [www.gezinsbond.be/veiligonline](http://www.gezinsbond.be/veiligonline) kan u leren hoe u MSN Messenger kan configureren om het communicatieproces van uw kinderen nog veiliger te maken.

Raadpleeg het verslag van Eurobarometer 2007 over Safer Internet for Children:  
[http://ec.europa.eu/information\\_society/activities/sip/eurobarometer](http://ec.europa.eu/information_society/activities/sip/eurobarometer)

# 3. Cyberpesten



## CYBERPESTEN

Communiceren via het internet en de mobiele telefoon heeft veel voordelen. Helaas zitten er ook kantjes aan die niet zo geweldig zijn: uw kinderen kunnen berichten ontvangen of versturen die hen of anderen kwetsen. Het is van belang dat u uw kinderen leert om zich altijd en overal te gedragen, ook online: zelfs onze eigen kinderen zijn niet altijd engeltjes ;-)

**Cyberpesten** is het gebruik van nieuwe informatie- en communicatietechnologieën om een individu of groep te pesten, te treiteren of te intimideren. Daarvoor kunnen e-mail, chat, instant messaging, gsm's of andere technologische hulpmiddelen worden gebruikt. In een virtueel spel kunnen pesters de **avatar** van uw kind aanvallen, bijvoorbeeld door deze te beschieten. Of ze kunnen de avatar dwingen om zich op een ongeweste manier te gedragen, of **virtuele bezittingen** stelen, .... Of iemand kan persoonlijke informatie openbaar maken, bijvoorbeeld door een persoonlijke foto of persoonlijke informatie op een openbaar forum of website te posten.

Dergelijk gedrag is net zo onaanvaardbaar als **pesten** op school of op de speelplaats. Ouders, leerkrachten en kinderen moeten hier dan ook aandacht voor hebben en er passend op kunnen reageren. In tegenstelling tot bij traditioneel pesten kan een kind zelfs gecyberpest worden als hij/zij niet direct in de buurt van de pesters is. De pesters kunnen bedriegende berichten via e-mail of sms sturen wanneer ze willen, dag en nacht.

U als ouders kan helpen om een omgeving te creëren waarin pesten niet wordt getolereerd: leer uw kinderen dat "anoniem" online zijn niet betekent dat zij zich onverantwoordelijk mogen gedragen. Kinderen moeten hun eigen rechten en verantwoordelijkheden kennen en weten hoe ze de rechten van anderen kunnen respecteren.

Zorg altijd voor een open dialoog tussen u en uw kinderen zodat u over eventuele verontwaardigende situaties kunt praten!

### HOOFDREGELS:

- Voorkom negatieve ervaringen door ervoor te zorgen dat uw kinderen weten hoe ze hun eigen privacy moeten beschermen en die van anderen moeten respecteren;
- Leer uw kinderen om niet te reageren op pestberichten;
- Help uw kinderen te begrijpen welke berichten en welk soort gedrag anderen kwetst en

hoe ze dit kunnen voorkomen;

- Zorg ervoor dat ze weten hoe ze mensen die hen vervelende berichten sturen in hun contactpersonenlijst kunnen blokkeren;
- Bewaar aanstootgevende berichten, u heeft ze misschien nog nodig als bewijsmateriaal;
- Ga na hoe de school van uw kinderen omgaat met pesten. Werk samen met andere ouders en leerkrachten om pesten en cyberpesten te voorkomen;
- Houd voeling met de omgeving van uw kinderen; leer hun vrienden, de ouders van hun vrienden, hun leerkrachten en hun klasgenoten kennen;
- Moedig uw kinderen aan om u over eventuele onaangename offline en online ervaringen te vertellen. Verzeker hen dat u voor ze klaarstaat, zelfs als ze ook zelf onvoorzichtig zijn geweest, en dat u samen met hen oplossingen zult zoeken!
- Zorg ervoor dat uw kinderen begrijpen dat het nooit hun schuld is als ze door iemand worden gepest.

## HANDIGE LINKS

Op [www.saferinternet.be](http://www.saferinternet.be) staat heel veel uitleg over wat cyberpesten is en hoe u er als ouder of leerkracht mee om kunt gaan.

<http://www.ond.vlaanderen.be/ict/ondersteuning/veiligICT>: Hier vindt u de brochure 'Veilig Online. Tips voor veilig ICT-gebruik op school' en de bijbehorende digitale lespakketten (op cd-rom), die door het Vlaams Departement Onderwijs en verschillende organisaties (waaronder Child Focus en het OIVO) ontwikkeld werden voor leerkrachten, directies en ICT-coördinatoren. Er is een heel hoofdstuk gewijd aan cyberpesten.

Klasse voor leerkrachten publiceerde een goed dossier over cyberpesten: zie <http://www.klasse.be/leraren/help.php?q=eerstelij>

[www.cyberpesten.be](http://www.cyberpesten.be) is een informatieve website over dit thema.

De Kinder- en jongerentelefoon biedt steun door middel van een telefonische en online hulpdienst. Kinderen en jongeren kunnen de KJT bereiken op het nummer 102 (gratis) en via [www.kjt.org](http://www.kjt.org).

[www.clicksafe.be](http://www.clicksafe.be) geeft informatie over het herkennen, voorkomen en aanpakken van cyberpesten aan zowel jongeren, ouders als leerkrachten.



## 4. Entertainment & downloaden



### HET IS NIET AL GOUD WAT BLINKT OP HET INTERNET

Het internet is een virtuele ruimte waar zich vele verschillende activiteiten afspelen, ook commerciële. Koopt u voor uw kinderen alle producten waar ze in de winkel om vragen of waarvoor ze reclame gezien hebben op televisie? Waarom leren we hen dan ook niet om op een slimme manier om te gaan met de producten en diensten waarvoor op het internet reclame gemaakt wordt? Voorbeelden zijn muziek en games, **ringtones**, en andere producten en diensten die je via het internet kan kopen.

Door samen met uw kinderen tijd door te brengen op het internet kunt u ze uitleggen dat producten als ringtones, **wallpapers**, **mp3's**, **avatars** etc. zelden gratis zijn. Als u er reclame voor ziet, wijs hen dan op de kleine lettertjes zodat ze leren dat ze niet alles op het **net** als vanzelfsprekend moeten aannemen.

Om u te abonneren op een dienst (al dan niet gratis), moet u vaak belangrijke persoonlijke informatie invullen op een **online formulier**. Vul dergelijke formulieren alleen in als u weet waarvoor die persoonlijke gegevens zullen worden gebruikt. Leer uw kinderen om zulke formulieren alleen samen met u in te vullen, nadat u zelf de gevolgen ingeschat hebt.

**Pop-up vensters** worden op het internet vaak gebruikt om dingen te verkopen. Ze zijn niet altijd slecht: het hangt ervan af of ze gelinkt zijn aan een betrouwbare website of niet. Over het algemeen kunt u de pop-up vertrouwen als u de website vertrouwt. Sommige pop-ups worden echter gebruikt om onbetrouwbare producten aan de man te brengen of leiden naar **online vragenlijsten** die gebruikt worden om persoonlijke gegevens te verzamelen. Leer uw kinderen om onbetrouwbare pop-ups te sluiten door op het rode kruisje rechtsboven in de hoek te klikken.

### ONLINE GAMEN

Kinderen kunnen games **spelen op een cd/dvd, op websites, gameconsoles of op gsm en andere draagbare apparatuur**.

**Online games verschillen van andere digitale spellen doordat er een actieve** netwerkverbinding voor **nodig is**. Deze spellen variëren van eenvoudige, bekende spellen als Pacman en Tetris tot virtual reality-spellen waarin verscheidene gebruikers samen online spelen en inhoud en verhalen creëren. Veel van zulke **multiplayer-spellen** hebben virtuele gemeenschappen, waar spelers met elkaar communiceren. Daarom gelden ook hier de tips over communiceren met onbekenden via het internet (zie het hoofdstuk over Communiceren).

Games spelen een belangrijke rol in de ontwikkeling van kinderen omdat hun sociale vaardigheden en hun vermogen tot strategisch denken zich ontwikkelen in een omgeving die begrensd wordt door spelregels. Veel digitale spellen zijn aantrekkelijk en interactief, en worden voor leerzame doeleinden gebruikt.

Maar niet alle digitale spellen zijn van goede kwaliteit. U moet zelf beslissen welke spellen het meest geschikt zijn voor uw kinderen. Door afspraken te maken, kunt u ervoor zorgen dat de tijd die uw kinderen doorbrengen met gamen niet ten koste gaat van andere activiteiten.

Er bestaat een pan-Europees leeftijdsclassificatiesysteem voor interactieve spellen, **PEGI online**, waarin spellen worden geclassificeerd op basis van leeftijd en inhoud.



Het systeem wordt zowel ondersteund door diverse fabrikanten, waaronder PlayStation, Xbox en Nintendo, als door uitgevers en ontwikkelaars van interactieve spellen in heel Europa. De inhoudspictogrammen van het systeem staan op de achterkant van de doos van de spellen die u voor uw kind koopt. Hou wel in gedachten dat de ene 12-jarige is de andere niet is.



## BESTANDEN DELEN & AUTEURSRECHT ©

Jongeren zien het internet vaak als een bron van films, muziek en spellen die ze kunnen downloaden, bekijken, beluisteren en spelen. Ze downloaden en uploaden vaak materiaal via **peernetwerken** zonder te beseffen dat het originele werk van artiesten of andere makers/**auteurs** beschermd wordt door het **auteursrecht**. Hier vallen zaken onder als films, liedjes, boeken, software en foto's.

### *Is het delen van bestanden illegaal?*

Het delen van bestanden is niet illegaal als die bestanden inhoud bevatten die u zelf heeft gemaakt, maar wel als u ze zelf enkel bewerkt hebt. Over het algemeen is het **uploaden** en downloaden van muziek en films zonder toestemming van de **rechthebbende** overal ter wereld illegaal (hoewel ieder land zijn eigen wetgeving heeft op vlak van auteursrecht). Als vuistregel geldt dat het delen van bestanden met muziek en films illegaal is en dat u heel voorzichtig moet zijn met **peer-to-peer** toepassingen.

### *Is het delen van bestanden riskant?*

Door **bestanden** te **delen** loopt uw computer gevaar: er worden poorten geopend via dewelke

kwaadaardige programma's en malware uw computer kunnen binnendringen, waardoor deze niet goed meer kan functioneren. Ook is het mogelijk dat anderen toegang krijgen tot uw persoonlijke gegevens of uw computer kunnen gebruiken om spam of illegale inhoud te versturen.

### *Waar vind ik legale muziek?*

Wereldwijd bieden honderden websites legaal muziek te koop aan, en soms zelfs gratis! Dit is bijvoorbeeld het geval op websites waar muzikanten hun fans alvast een voorproefje van hun werk willen geven en hen op de hoogte willen houden van hun concerten en albums.

## HOOFDREGELS

- Gebruik legale sites om muziek en films te downloaden van het internet;
- Moedig uw kinderen aan om websites met legale inhoud te gebruiken en leg hen uit dat niet alles is wat het lijkt op het internet;
- Leg uit wat de risico's zijn van het onvoorzichtig downloaden van materiaal;
- Zorg dat uw computer is beveiligd en gebruik altijd een up-to-date antivirusprogramma;
- Leer uw kinderen om legaal gedownloadte bestanden op te slaan op de harde schijf en ze eerst te scannen voor ze te openen;
- Lees altijd eerst de privacyverklaring en de gebruiksvoorwaarden voordat u iets installeert. Controleer of de software van het programma dat u wilt downloaden betrouwbaar is;
- Sluit onbetrouwbare pop-up vensters door op het rode kruisje rechtsboven in de hoek te klikken. Klik ze niet aan.

## KINDEREN & GAMES:

- Maak afspraken met uw kind over de speelduur;
- Zet de computer of spelconsole in een gezamenlijke ruimte, zodat u een oogje in het zeil kan houden.
- Hou toezicht op de speelgewoonten van uw kinderen: als u ze op de speelplaats in de gaten houdt, waarom dan ook niet als ze spelen op virtuele plaatsen?
- Bespreek de inhoud van het spel: welke elementen zijn realistisch en welke niet, wat vinden ze leuk?
- Zorg dat u, voordat u een spel voor uw kinderen koopt, zeker bent dat de inhoud geschikt

is voor hun leeftijdscategorie (pan-Europees PEGI-systeem of een nationaal classificatiesysteem).

*Als uw kinderen online games met meerdere gebruikers spelen:*

- Kies sites met strenge regels en echte moderators;
- Spreek met uw kinderen af dat ze geen persoonlijke gegevens aan andere spelers geven;
- Druk ze op het hart niet offline af te spreken met andere spelers zonder dat u erbij bent;
- Moedig uw kinderen aan om melding te maken van zaken als pesten, bedreigingen of ongepast taalgebruik, het tonen van onaangename inhoud of uitnodigingen om ook offline af te spreken;
- Laat uw kind stoppen met het spel of verander het online ID van uw kind als u zich ongemakkelijk voelt door een bepaald spelelement of de manier waarop het spel zich ontwikkelt.

## HANDIGE LINKS

Meer info over slim consumeren, consumentenbedrog op internet, de commerciële doeleinden van veel kinder- en jongerensites, kopen en reclame online, downloaden, auteursrecht, ... vind je op de volgende sites:

[www.saferinternet.be](http://www.saferinternet.be)

[www.oivo.be](http://www.oivo.be)

[www.consumentenbedrog.be](http://www.consumentenbedrog.be)

[www.test-aankoop.be](http://www.test-aankoop.be)

<http://mineco.fgov.be/>

[http://www.eccbelgium.be/default\\_NL.asp](http://www.eccbelgium.be/default_NL.asp)

<http://www.mijnkindonline.web-log.nl/>

Speel ook ‚Spotm‘nblog‘ op [www.saferinternet.be](http://www.saferinternet.be). In dat spel en in het bijbehorende pedagogische dossier voor ouders en leerkrachten vind je meer info over deze aspecten van het internet. Op dezelfde site staat ook meer info over verschillende aspecten van e-gaming.

Kom meer te weten over online games en het PEGI-**leeftijdsclassificatiesysteem**:

<http://www.pegionline.eu>

Kijk ook eens op [www.weetwatzegamen.nl](http://www.weetwatzegamen.nl) en de bijbehorende weblog waar u als ouder informatie kunt vinden over games en ervaringen met andere ouders kan delen.

Een lijst van websites van over de hele wereld waar u legaal muziek kan kopen:

<http://www.pro-music.org>



C. Oplossingen bij de voorgestelde activiteiten

# 1. Beveiligd en wel



## ACTIVITEITEN MET AANTEKENINGEN

Zet de woorden bij de juiste afbeelding: Computerkast, muismat, beeldscherm, luidsprekers, webcam, printer, USB-stick (of geheugenstick), muis, CD-Rom.

*Een opwarmingsoefening om uw kinderen vertrouwd te maken met de verschillende onderdelen van de computer en andere aanverwante hardware. U kunt dit naar wens verder uitbreiden.*

Vraag aan je ouders of ze je een e-mail met een **bijlage** kunnen sturen, of stuur er een aan jezelf. Oefen het volgende: klik met de rechtermuisknop op de bijlage en sla hem op op het bureaublad van je computer. Ga naar je bureaublad, klik met de rechtermuisknop op het document en klik op **scan**. Als je zeker weet dat het document veilig is, kun je het openen. Dus: Rechtermuisknop en dan OPSLAAN – SCANNEN – OPENEN.

*Stuur een e-mail naar het e-mailadres van uw kind of naar uw eigen e-mailadres en voeg een bijlage toe. Laat uw kind de instructies van de oefening volgen om het document op te slaan door er met de rechtermuisknop op te klikken zonder het te openen. Nadat het bestand op het bureaublad of in een map zoals Mijn Documenten is opgeslagen, kan u uw kind tonen hoe het*

*dit bestand moeten scannen alvorens het te openen door er nogmaals met de rechtermuisknop op te klikken. Stimuleer dergelijke veilige gewoontes bij uw kind.*

Volg Laura's advies op en leer hoe je je **e-mailadres** moet uitschrijven als je het echt eens online moet zetten. Zo voorkom je dat je e-mailadres automatisch wordt opgepikt en gebruikt door spammers.

Voorbeeld: cybercat.smith@mymail.com = cybercat punt smith apenstaartje mymail punt com

Schrijf om te oefenen de e-mailadressen van jullie gezin eens uit: *je eigen e-mailadres, e-mailadres van jullie gezin, e-mailadres van je moeder, e-mailadres van je vader*

*Om te voorkomen dat uw e-mailadres automatisch door software wordt opgepikt en gebruikt wordt voor de verspreiding van spam, kunt u het helemaal uitschrijven in plaats van het letterlijk over te nemen. Laat uw kinderen oefenen met de hierboven beschreven techniek. Onthoud echter dat uw kinderen hun e-mailadres best helemaal niet op het internet zetten, en als ze dat toch doen, ze een e-mailadres moeten gebruiken dat **niet** hun volledige naam onthult (zie hoofdstuk Communiseren).*

Help Emma een handje om dit allemaal te begrijpen voordat Laura verder gaat: kijk naar de activiteiten in het vak en omcirkel de dingen die je alleen kunt doen als je bent aangesloten op het internet.

*Voor heel jonge kinderen is het wellicht niet helemaal duidelijk voor welke activiteiten een netwerkaansluiting nodig is en voor welke niet. Voor het schrijven van een tekst hoeft de pc niet aangesloten te zijn op het internet, maar om te chatten wel. U kunt op uw pc naar muziek luisteren via een cd of een muziekbestand dat staat opgeslagen op uw computer, maar u kunt ook online naar muziek luisteren. Uw kinderen moeten alleen die activiteiten omcirkelen waarvoor een netwerkaansluiting nodig is.*

Typ samen met je ouders [www.google.be](http://www.google.be) in op je browser. Zoek informatie op over de Tyrannosaurus Rex, en probeer uit te vinden wanneer deze dinosaurus op aarde leefde. Zoek ook een mooie afbeelding van een Tyrannosaurus. Vergeet niet om de informatie op drie verschillende websites met elkaar te vergelijken en te controleren.

*Leer uw kinderen goede zoekgewoonten aan door hen eraan te herinneren dat ze niet alles moeten geloven wat ze online zien. Herinner hen eraan om informatie te zoeken en te vergelijken op minstens drie sites en altijd hun bronnen te vermelden als ze een schoolopdracht maken.*

Typ samen met je ouders [www.google.be](http://www.google.be) in op je browser. Zoek op een bepaald onderwerp, bijvoorbeeld Tyrannosaurus Rex, en sla de drie sites die je het interessantst vindt op door bovenaan de browserpagina op het menu Favorieten te klikken en ze toe te voegen aan jouw favoriete sites. Je kan ook je eigen map aanmaken.

*Door interessante sites in de map Favorieten (optie in de browserwerkbalk) op te slaan en te ordenen, moeten uw jonge kinderen minder snel gebruik maken van zoekmachines om informatie op te zoeken op het internet.*

## ALLES OP EEN RIJTJE

1: (beveiligd) 2: (virus),(onbekende), (downloaden), (geïnficeerde),(geheugenstick), (onbeveiligde) 3: (vreemd) 4: (kent),(bijlagen), (onderwerpen), (spam) 5: (spam), (enkel) 6: (eerste), (drie),(vergelijk),(iedereen), (zetten) 7: (antivirus-), (antispyswareprogramma's) 8: (praat), (ouders) 9: (zeg)

### VOORGESTELDE OPLOSSINGEN BIJ DE SITUATIEKAARTJES

**SITUATIE 1.** Surf nooit op het internet als je computer niet beveiligd is met antivirus- en antispyswareprogramma's die up-to-date zijn. Dat is net zoals als een grens zonder grenswachten; je computer kan dan worden geïnficeerd met schadelijke programma's zoals virussen, Trojaanse paarden, wormen of spyware.

**SITUATIE 2.** Let goed op met e-mails van mensen die je niet kent en die bijlagen bevatten of met 'veelbelovende' e-mails, want dat is hoogstwaarschijnlijk spam! Spam kan je computer infecteren met schadelijke programma's zoals virussen, Trojaanse paarden, wormen of spyware. Open zulke e-mails niet. Blokkeer in plaats daarvan de afzender door met de rechtermuisknop op het bericht te klikken en 'Afzender blokkeren' te selecteren, of verwijder ze simpelweg.

**SITUATIE 3.** Als je op het internet informatie opzoekt, vertrouw dan niet meteen de eerste de beste pagina die je te zien krijgt. Bekijk minstens 3 andere sites en vergelijk de informatie die erop staat. Denk eraan: iedereen met toegang tot het internet kan informatie schrijven en die op het net zetten. Als je een opstel of spreekbeurt maakt, moet je altijd de bron vermelden van de informatie en de afbeeldingen die je gebruikt hebt... net als een echte wetenschapper.

## 2. Communiceren LoL ;-D



### ACTIVITEITEN MET AANTEKENINGEN

Geef aan hoe persoonlijk de volgende zaken voor jou zijn: Je telefoonnummer, De kleur van je haar, Je naam, Het land waar je woont, De naam van je school, Je adres, De naam van je huisdier, Het beroep van je ouders, Je e-mailadres, Je foto's, Je leeftijd.

*Hebben uw kinderen dezelfde voorstelling van privacy als u? De drie kleuren staan voor zeer persoonlijke (rood), vrij persoonlijke (oranje) en niet zo persoonlijke (groen) informatie.*

Help Emma een heel goed wachtwoord te maken met behulp van Laura's tips.

*Goede wachtwoorden zijn opgebouwd uit een willekeurige reeks verschillende tekens (cijfers, letters en leestekens) en moeten altijd geheim worden gehouden.*

Volg Emma's voorbeelden en maak een veilig profiel. Maak daarna een voorbeeld van een profiel dat niet veilig is.

*Laat uw kinderen een veilig profiel maken en vervolgens een minder veilig profiel waarop wel persoonlijke informatie staat. Herinner uw kinderen eraan dat het maken van een veilig profiel hen niet beschermt wanneer ze hun privacy ook niet blijven beschermen als ze online communiceren.*

Kijk goed naar deze foto en schrijf op wat je nu over deze persoon weet:

*Welke persoonlijke informatie kan je uit een foto halen? Kinderen zijn zich vaak niet bewust van de invloed en kracht die afbeeldingen hebben.*

'Ga door op Emma's idee en bedenk 3 adviezen die "Alex Rood-truien-kapje" zou krijgen van Laura om zichzelf tegen "webwolven" te beschermen?

*Ga na of uw kinderen beseffen dat contact leggen met vreemden op het internet riskant kan zijn.*

Hoe zou je online door anderen behandeld willen worden? (1..... 2..... 3.....)

*Zorg dat uw kinderen begrijpen dat ze anderen net zo moeten behandelen als ze zelf behandeld willen worden...*



ONTCIJFER DE CODE: Ontdek wat deze populaire chatacroniemen betekenen.

*Verbeter uw kennis van acroniemen door het hoofdstuk Communiceren/nettiquette, chattaal te raadplegen.*

Gebruik toetsencombinaties om deze emoticons uit te beelden: Smiley – Verdrietig gezichtje – Knipogend gezichtje – Verbaasd gezichtje – Brede lach – Tong uitsteken

*Zie hoofdstuk Communiceren/nettiquette voor meer informatie*

## ALLES OP EEN RIJTJE

1: (profiel) 2: (privacy), (verantwoordelijk) 3: (mensen die je niet kent), (zeg) 4: (Nettiquette), (behandeld) 5: (emoticon) 6: (wachtwoord), (leestekens) 7: (geheim) 8: (weiger) 9: (kent)

### VOORGESTELDE OPLOSSINGEN BIJ DE SITUATIEKAARTJES

**SITUATIE 4.** Als je op het internet actief bent, kan jouw profiel, of de informatie die je over jezelf geeft, wel tientallen, honderden, duizenden of zelfs miljoenen mensen bereiken. Daarom is het belangrijk om de informatie die je over jezelf geeft zorgvuldig te kiezen en er goed over na te denken. Geef persoonlijke informatie alleen aan mensen die je vertrouwt en die je in de offline wereld ook goed kent en laat je naam, leeftijd adres, school, sportclub,... nooit achter op een weblog een website of in een chatbox.

**SITUATIE 5.** Waarschijnlijk heeft Mike het wachtwoord van zijn e-mail ook aan zijn vriend gegeven. Die wilde hem vervolgens een hak zetten door in Mike's naam gemene e-mails te sturen. Geef wachtwoorden nooit aan anderen, tenzij je het niet erg vindt dat andere mensen jouw e-mail lezen of net doen of ze jou zijn en dingen zeggen die jij nooit zou zeggen!

**SITUATIE 6.** Afspreken met een vreemde is niet verstandig. Maar als je echt denkt dat je een online vriendje of vriendinnetje dat jou wil ontmoeten goed kunt vertrouwen, vertel het dan aan je ouders en zorg dat een van hen met je meegaat. Spreek af op een openbare plaats. Een echte vriend of vriendin met goede bedoelingen zal dat niet erg vinden. Alleen mensen die iets te verbergen hebben, vinden dat erg.

# 3. Cyberpesten



## ACTIVITEITEN MET AANTEKENINGEN

Maak een tekening van de uitnodiging die Alex van zijn leerkrachten heeft gekregen. Teken ook het antipestlogo en de slogan die de school gebruikt voor de antipestweek.

*Uw kinderen mogen hun creativiteit uitleven in het lege vak.*

Volg Alex' voorbeeld en geef vijf redenen waarom je iemand een "rode kaart" zou geven.

*Besprek met uw kinderen welk gedrag zij onaanvaardbaar vinden.*

## ALLES OP EEN RIJTJE

1: (fair), (bederven) 2: (praat) 3: (enkele) 4: (cyberpesten) 5: (blokkeer) 6: (ken) 7: (reageren)

### VOORGESTELDE OPLOSSINGEN BIJ DE SITUATIEKAARTJES

**SITUATIE 7.** Je gsm op deze manier gebruiken, kan echt niet door de beugel. Verspreid geen berichten, beelden of ander materiaal dat kwetsend kan zijn. Behandel anderen altijd zoals jij zelf graag behandeld zou willen worden. Praat er in zo'n geval altijd over met je ouders of een andere volwassene die je vertrouwt.

**SITUATIE 8.** Alex moet zijn vriend vertellen dat het nare gedrag van degene die hem pest niet zijn schuld is. Hij moet niet op de pestberichten reageren, maar ze bewaren als bewijs en ze aan zijn ouders of leerkrachten laten zien. Ook Alex moet hier met zijn ouders over praten: zij kunnen hem helpen zijn vriend bij te staan.

**SITUATIE 9.** Netiquette wil zeggen dat je anderen op het web net zo behandelt als jij graag behandeld zou willen worden. We zijn ervan overtuigd dat je hier nu genoeg over hebt geleerd om Emma met deze opdracht te kunnen helpen.

# 4. Entertainment & Downloaden



## ACTIVITEITEN MET AANTEKENINGEN

Open je favoriete zoekmachine. Typ “gratis ringtones” of “gratis games” in, en wacht af wat je krijgt. **Kijk op enkele websites. Kun je valkuilen ontdekken?**

*Oefen door te zoeken met de gegeven zoektermen en controleer de websites die je krijgt op marketingvalkuilen. Merk op dat de informatie die verstopt zit in de kleine lettertjes wordt weggelaten in de reclameslogans.*

Wat is jouw favoriete computerspel? Kijk of je ouders het spel ook kennen en of ze het kunnen beschrijven. Als ze geen idee hebben, leg het dan eerst uit, en laat ze vervolgens een korte beschrijving van het spel maken. Hebben ze het goed gedaan? Hoeveel punten op tien krijgen ze? .../10. Ouder schrijft hier een samenvatting van de favoriete game van het kind. Het kind maakt er een tekening van.

*Weet u werkelijk wat voor soort spellen uw kinderen online spelen, en weet u welk spel hun lievelingsspel is? Laat hen uw kennis op de proef stellen!*

## ALLES OP EEN RIJTJE

1: (gratis) 2: (formulieren) 3: (val) 4: (illegale) 5: (kruisje) 6: (negeren) 7: (privacy) 8: (zelf), (delen) 9: (download)

## VOORGESTELDE OPLOSSINGEN BIJ DE SITUATIEKAARTJES

**SITUATIE 10.** De meeste muziek en films die op het internet staan, zijn in feite illegale kopieën. Bovendien wemelt het op websites waar mensen muziek en films delen meestal van de schadelijke programma's zoals virussen, Trojaanse paarden, wormen of spyware. Emma kan het beste voor oplossing b of c kiezen. Natuurlijk is het veel goedkoper voor haar om haar favoriete liedje te downloaden van een betrouwbare website met legale muziek dan om de hele cd te kopen. Ze moet haar ouders om hun mening en toestemming vragen.

**SITUATIE 11.** Er bestaan wel gratis diensten op het internet, maar ringtones, wallpapers, mp3's, avatars en dat soort dingen zijn zelden gratis. Als Alex nog eens goed op die website kijkt, ontdekt hij waarschijnlijk een stel heel kleine lettertjes, waarin de werkelijke kosten van de diensten staan vermeld. Met ringtones, quizzen, games, etc. kun je uitstekend mensen verleiden om zich te abonneren op zogenaamde 'gratis' diensten die in werkelijkheid geld kosten. Die abonnementen kan je bovendien vaak zeer moeilijk opnieuw opzeggen.

**SITUATIE 12.** Alex moet eraan denken om zijn identiteit geheim te houden als hij online speelt met mensen die hij in het echt niet kent. Hij mag geen informatie geven over zijn woonplaats, school, achternaam etc. Ook moet hij zijn ouders vertellen welke games hij speelt en mag hij nooit een game van het internet downloaden zonder dat eerst aan zijn ouders te vragen, want dat zou de computer kunnen beschadigen.



## D. Glossarium

**Aanmelden:** zich abonneren op een online-dienst: een nieuwsbrief, discussieforum, e-mail, chatplatform etc. Normaal moeten gebruikers de optie krijgen om zich opnieuw uit te schrijven als ze dat willen.

**Abonneren:** zich vrijwillig inschrijven bij een dienst of nieuwsbrief waardoor informatie direct naar de inbox van uw persoonlijke postvak wordt gestuurd.

**Account:** door een account wordt uw authenticiteit bevestigd en bent u bevoegd om via een gebruikersnaam en wachtwoord gebruik te maken van online-diensten. U kunt met het besturingssysteem voor elk gezinslid een aparte gebruikersaccount maken.

**Acroniem:** een afkorting die bestaat uit de eerste letters van elk woord uit een zinsdeel of uitdrukking. Acroniemen worden vaak gebruikt door chatters om sneller te kunnen communiceren, bijv. LoL, CU, Btw (zie hoofdstuk communiceren).

**Alarmsignaal:** een venstertje dat op het scherm verschijnt en dat informatie of een waarschuwing voor een mogelijk schadelijke handeling bevat, bijv. nieuwe e-mail of de stand van zaken met betrekking tot uw antivirusprogramma.

**Antispywareprogramma:** een programma dat spyware bestrijdt. Het programma scant alle inkomende gegevens op spywaresoftware en blokkeert vervolgens de bedreigingen die het tegenkomt of geeft een lijst waaruit u verdachte elementen kunt verwijderen.

**Antivirusprogramma:** een computerprogramma dat computervirussen en andere schadelijke software identificeert, isoleert, blokkeert en vernietigt. Het antivirusprogramma scant de bestanden eerst op bekende virussen en identificeert dan verdacht gedrag van computerprogramma's die aangeven geïnfecteerd te zijn.

**Auteur:** de maker van een literair of audiovisueel werk, software etc. Auteursrecht beschermt het werk van de auteur tegen illegale reproductie.

**Blog:** Auteursrecht: een serie exclusieve rechten die het gebruik van een idee, werk of informatie regelen. Auteursrecht wordt weergegeven met het symbool „©“.

**Avatar:** het profiel van een gebruiker dat wordt weergegeven met een gebruikersnaam en een afbeelding, icoontje of een 3D-personage in online-computergames en virtuele werelden.

**Bestanden delen:** het online uitwisselen van bestanden tussen computergebruikers. De term beslaat zowel het aanbieden van bestanden aan andere gebruikers (uploaden) als het kopiëren van beschikbare bestanden van het internet naar een computer (downloaden). Meestal worden de bestanden uitgewisseld via P2P ('peer-to-peer')-netwerken.

**Bestanden verzenden:** het versturen van bestanden via een computernetwerk. Vanuit het oogpunt van de gebruiker wordt het verzenden van bestanden vaak aangeduid als uploaden of downloaden.

**Besturingssysteem:** een programma dat de fundamentele functies van een computer uitvoert, waardoor andere programma's kunnen draaien. Bekende voorbeelden zijn Windows, Linux en Mac OS.

**Bewerken:** het veranderen van een afbeelding, bestand, foto of illustratie op een duidelijke of minder duidelijke manier. Tegenwoordig zijn er vele hulpmiddelen die kunnen worden gebruikt om de inhoud of vorm van gegevens te beïnvloeden, wat leidt tot een van het origineel afwijkend resultaat.

**Bijlage:** een computerbestand dat met een e-mailbericht wordt meegestuurd. Wormen en virussen worden vaak verspreid via e-mailbijlagen. E-mails van onbekende afzenders met bijlagen moeten als verdacht worden beschouwd.

**Blog:** afkorting van weblog. Een website waarvoor een individu of groep inhoud genereert, meestal dagelijks, die bestaat uit teksten, foto's, audiovisuele bestanden en links.

**Bloggen:** het schrijven op of bijwerken van een (web)blog.

**Browsen:** het gebruiken van een browser om websites te bekijken of gewoon op het internet te surfen.

**Browser:** een programma voor het bekijken van websites. Internet Explorer, Netscape Navigator en Firefox zijn enkele van de meest gebruikte browsers voor Windows, terwijl Safari gangbaar is voor Macs. De meest recente versies van deze browsers bevatten vernieuwende functies voor ouderlijk toezicht.

**Cd-rom:** een acroniem voor 'compact disc read-only memory'. Het is een niet-opneembare compact disc met voor een computer leesbare gegevens. Cd-roms worden vaak gebruikt om computersoft-

ware te distribueren.

**Chatten:** synchrone communicatie via het internet door middel van geschreven berichten, door gebruik te maken van chat- en instant messaging-toepassingen (bijv. MSN).

**Chatroom:** openbare virtuele ruimte voor directe communicatie. Mensen uit de hele wereld kunnen elkaar ontmoeten in chatrooms en met elkaar praten door berichtjes te typen. Als uw kinderen een chatroom bezoeken, zorg er dan voor dat die geschikt is voor hun leeftijd en er toezichthouders en moderators aanwezig zijn.

**Computerbestand:** een archief/verzameling van gerelateerde informatie (documenten, programma's etc.) opgeslagen op een computer onder een eigen bestandsnaam. Computerbestanden kunnen worden gezien als de moderne tegenhanger van papieren documenten die op kantoor en in de bibliotheek in dossiermappen werden bewaard.

**Computerprogramma:** meestal software genoemd. Software bestaat uit een gestructureerde reeks instructies, geschreven door computerprogrammeurs, waardoor computers taken kunnen uitvoeren. Als je een softwareprogramma koopt, staat dat meestal op een cd-rom (zie definitie).

**Contactpersonenlijst:** een verzameling contactpersonen in instant messaging en e-mailprogramma's, online games, mobiele telefoons etc. Contactpersonen kunnen worden toegevoegd, geweigerd en verwijderd.

**Cookies:** een bestand dat door een website op uw computer wordt gezet. Telkens als u de website bezoekt, wordt de cookie teruggestuurd naar de server waarop de website is opgeslagen. Cookies rapporteren uw sitevoorkeuren en worden gebruikt door online-winkels. Het weigeren van cookies kan bepaalde websites onbruikbaar maken.

**Cyberpesten:** pesten via elektronische media, meestal via instant messaging en e-mail. Het kan bestaan uit herhaaldelijk toegebrachte schade, bedreigingen, seksueel getinte opmerkingen en kleinerend taalgebruik. Cyberpesters kunnen persoonlijke contactinformatie van slachtoffers publiceren en zelfs hun identiteit aannemen om in hun naam materiaal te publiceren met de bedoeling hen belachelijk te maken.

**Digitaal spel:** een spel gemaakt door spelontwerpers dat gespeeld kan worden op een computer. Een online game wordt omschreven als een digitaal spel waarvoor een actieve netwerkverbinding nodig is om het te kunnen spelen. Online games kunnen interactie tussen meerdere spelers ondersteunen.

**Directory:** een organisatie-eenheid die uw computer gebruikt om mappen en bestanden in een hiërarchische structuur te ordenen, bijv. Mijn Documenten, Mijn Afbeeldingen etc.

**Downloaden:** het proces van het kopiëren van een bestand van een online-dienst naar een computer.

**E-mail:** een middel van elektronische schriftelijke communicatie waarmee u berichten met allerlei computerbestanden als bijlage kunt versturen: tekst, foto's, audio en meer.

**E-mailadres:** een virtuele locatie waarop e-mailberichten kunnen worden bezorgd. Een e-mailadres bestaat uit twee delen gescheiden door het @-symbool.

**Emoticon:** een afbeelding, icoontje om gevoelens en emoties over te brengen, bijv. een smiley. Het symbool kan worden gemaakt met gewone toetsenbordtekens en leestekens of met kant-en-klare tekens van chatrooms, gamerooms, instant messaging-diensten, mobiele telefoons etc.

**Favorieten:** een aan te passen browsermap waarin u interessante links kunt opslaan. De links kunnen worden geordend in subfolders en/of gemerkt worden met trefwoorden zodat u ze makkelijk terug kunt vinden.

**Filter:** toepassing die de toegang tot informatie of specifieke internetdiensten regelt, voor twijfelachtige websites waarschuwt, de zoekgeschiedenis van de gebruiker bijhoudt, risicovolle sites blokkeert en de computer zelfs helemaal uitschakelt. Filtersystemen kunnen geïnstalleerd worden op autonome computers, servers, telefoons met toegang tot het internet etc.

**Firewall:** een hardware- (geïntegreerd in uw router) of software- (geïnstalleerd op uw pc) hulpmiddel dat is geconfigureerd om te voorkomen dat onbevoegde gebruikers (zoals hackers en krakers) toegang krijgen tot een op het internet aangesloten computer of computernetwerk.

**Flaming:** vijandige en beledigende interactie tussen internetgebruikers. Het doet zich meestal voor op discussieforums, Internet Relay Chat (IRC) of zelfs via e-mail.

**Formulier (online formulier):** een geformatteerd document met lege velden waarin u gegevens kunt invullen. Het elektronische formulier kan worden ingevuld met vrije tekst of door opties te kiezen uit vooraf opgestelde lijsten (dropdownmenu). Nadat u het formulier hebt ingestuurd, worden de gegevens meteen naar een verwerkingstoepassing gestuurd die de informatie in een database zet.

**Forum:** een online-discussiegroep waar deelnemers met gezamenlijke interesses vrijuit berichten over diverse onderwerpen kunnen uitwisselen.

**Freeware en shareware:** software wordt over het algemeen beschermd door auteursrecht en mag daarom niet gratis gedownload worden. Freeware betekent dat de houder van het auteursrecht toestaat dat iedereen de software gratis kan gebruiken. Shareware betekent dat de houder van het auteursrecht toestaat dat iedereen de software kan gebruiken voor een bepaalde proefperiode. Na die periode moet de gebruiker een vergoeding betalen om van de dienst gebruik te mogen blijven maken.

**Gebruikersprofiel:** een reeks gegevens die een specifieke gebruiker van software, een website of andere technische hulpmiddelen beschrijft. Het profiel bevat meestal persoonlijke informatie als gebruikersnaam en andere details (bijv. geboortedatum, interesses).

**Geheugen-/USB-stick:** apparatuur met een USB-aansluiting ('universal serial bus') om gegevens op te bewaren. Een geheugenstick is meestal klein, licht, verwijderbaar en overschrijfbaar.

**Gezinsinstellingen:** ook wel ouderlijk toezicht genoemd. Instellingen die worden gebruikt om browsers of andere webtools kindvriendelijker te maken door middel van functies als inhoudsfilters, speeltijdbeperking, spelbeheer etc.

**GSM:** een elektronisch telecommunicatieapparaat, ook wel mobiele telefoon, draagbare telefoon, mobiel, smartphone of zaktelefoon genoemd. Het heeft dezelfde basiscapaciteiten als een traditionele vaste telefoonlijn. Tegenwoordig zijn de meeste gsm's uitgerust met een camera en hebben vele



toegang tot het internet.

**Hacker:** populaire term voor iemand die zich met het kraken van computers bezighoudt (zie 'kraker'). Wordt in computerkringen ook gebruikt om een computerfanaat aan te duiden.

**Hardware:** het tastbare deel van een computer, in tegenstelling tot de computersoftware die taken uitvoert binnenin de hardware. Het kan intern zijn: moederbord, harde schijf en RAM, vaak componenten genoemd; of extern: monitor, toetsenbord, printer etc., ook wel randapparatuur genoemd.

**Homepage:** de webpagina die automatisch geladen wordt als een webbrowser opstart. De term wordt ook gebruikt om naar de voorpagina of belangrijkste webpagina van een website (zie definitie) te verwijzen.

**Hulplijn:** een e-mail- en soms ook telefoondienst die kinderen hulp biedt. Kinderen kunnen op die manier hun zorgen uiten over illegale en schadelijke inhoud en onaangename of enge ervaringen met betrekking tot het gebruik van online technologieën.

**Identiteitsdiefstal:** het stelen van persoonlijke gegevens (bijv. naam, geboortedatum, creditcardnummer) en die op illegale wijze gebruiken.

**Illegale inhoud:** online inhoud die volgens nationale wetgeving illegaal is. Voorbeelden hiervan zijn beelden van seksueel misbruik van kinderen of websites die aanzetten tot haat of racisme.

**Instant Messaging (IM):** een vorm van directe en gelijktijdige elektronische communicatie tussen twee of meer gebruikers. Via IM kunt u communiceren met een geselecteerde lijst contactpersonen. Als personen van uw contactpersonenlijst online zijn, wordt u dit meteen gemeld.

**Internet:** een wereldwijd, openbaar toegankelijk netwerk van onderling verbonden computernetwerken. Via dit netwerk worden gegevens verstuurd en uitgewisseld. Het bestaat uit kleinere thuis-, universiteits-, zaken- en overheidsnetwerken die diverse diensten uitvoeren, zoals informatie verspreiden, e-mails, online chatten, bestanden versturen etc.

**Internetaansluiting:** de middelen waarmee gebruikers aansluiten op het internet. Veel voorkomende manieren van internetaansluiting zijn o.a. via inbellen, T-lines, WiFi, satelliet en mobiele telefoon.

**Junkmail:** ongewenste e-mailberichten. Aangezien het internet openbaar is, kan er maar weinig worden gedaan om junkmail te voorkomen, net zoals het onmogelijk is spam te voorkomen.

**Junkmail-/Spammap:** de plaats in een e-mailpostvak, waar e-mails die als spam of junkmail worden beschouwd, worden opgeslagen.

**Kinderporno:** kinderporno heeft in verschillende landen verschillende wettelijke definities. Kinderporno wordt minimaal omschreven als een afbeelding van een kind dat expliciete seksuele handelingen verricht of wordt afgebeeld alsof hij of zij expliciete seksuele handelingen verricht.

**Kraken:** het illegaal kopiëren van commerciële software door de auteursrechtelijke beschermingsfunctie te breken.

**Kraker:** iemand die illegaal inbreekt in computersystemen.

**Link:** een referentie naar een online document (webpagina, tekstdocument, foto etc.). Als u de link aanklikt, gaat u naar een nieuwe pagina of een andere website. Tekstlinks zijn meestal blauw van kleur en onderstreept, maar ze kunnen ook andere kleuren hebben en niet onderstreept zijn. Beelden kunnen ook dienen als link naar andere webpagina's.

**Malware:** afkorting van 'malicious software' (kwaadaardige software), staat voor software die is ontworpen om een computer binnen te dringen of te beschadigen zonder dat de eigenaar daarvan op de hoogte is en er toestemming voor heeft gegeven. Het omvat computervirussen, wormen, Trojaanse paarden, spyware, oneerlijke adware en andere schadelijke en ongewenste software.

**Map:** een eenheid in een bestandensysteem dat een groep bestanden en/of andere directories bevat. Mappen kunnen meerdere documenten bevatten en worden gebruikt om informatie te ordenen.

**Massively Multiplayer Games:** games met een rijke 3D-wereld die wordt gebruikt door duizenden gamers in de rol van fictionele personages die tegen elkaar strijden. Role playing games zijn toonaangevend in deze categorie: de deelnemers creëren of volgen gezamenlijk een verhaal.

**Meldpunt:** telefonische hulplijn of webdienst waar mensen terecht kunnen met klachten over (vermeende) illegale inhoud en/of illegaal gebruik van het internet. Meldpunten moeten effectieve, transparante procedures hanteren om de klachten te behandelen en de steun genieten van de regering, industrie, wetshandhavingdiensten en internetgebruikers in de landen waar ze actief zijn.

**Mp3:** code-opmaak specifiek voor audio. Een mp3-bestand neemt ongeveer een tiende van de ruimte van het oorspronkelijke audiobestand in beslag, maar het geluid is bijna van cd-kwaliteit. Vanwege hun kleine formaat en goede geluid zijn mp3-bestanden uitgegroeid tot een populaire manier om muziekbestanden op te slaan op zowel computers als draagbare apparatuur.

**Net:** afkorting voor het internet.

**Nettiquette:** internetetiquette die beleefdheidsregels voor online-communicatie voorschrijft.

**Nickname:** synoniem van schermnaam en bijnaam of pseudoniem. Deze naam vertegenwoordigt de gebruiker van een online dienst en wordt gekozen door de gebruiker zelf. Nicknames worden ook gebruikt in contactpersonenlijsten, chatrooms etc. Uw nickname, mits goed gekozen, kan uw anonimiteit online beschermen.

**Nieuwsgroep:** zie definitie forum.

**Ouderlijk toezicht:** zie definitie gezinsinstellingen.

**Persoonlijke gegevens:** alle informatie die met een persoon in verband kan worden gebracht. Als er persoonlijke gegevens worden verzameld, verwerkt en opgeslagen, moeten de redenen daarvoor expliciet vermeld worden.

**Pesten:** het herhaaldelijk toebrengen van schade, uiten van bedreigingen, maken van seksueel getinte opmerkingen, overgaan tot fysieke aanvallen en kleinerend taalgebruik, begaan door een of meer pesters.

**Poort:** een interface op een computer waarmee die kan worden aangesloten op andere apparatuur. Poorten kunnen intern of extern zijn. Interne poorten maken verbinding met een diskdrive of

netwerk, terwijl externe poorten verbinding maken met randapparatuur zoals een printer of toetsenbord.

**Pop-up venster:** een venster dat plotseling verschijnt als u een website bezoekt of een speciale functie-toets indrukt. Doorgaans bevatten pop-up vensters een menu met commando's en blijven ze op uw scherm staan totdat u één van de commando's selecteert of het venster sluit door op het kruisje in de rechterbovenhoek te klikken.

**Privacy:** het vermogen van een individu of groep om de informatiestroom over zichzelf te reguleren en zich zo selectief te kunnen blootgeven. Privacy wordt soms geassocieerd met anonimiteit, de wens om onopgemerkt te blijven in de openbare wereld.

**Privacyinstelling:** een serie accountspecifieke privacydetails die u kunt aanpassen om uw privacy beter te kunnen beschermen tegen onthulling van persoonlijke informatie, cookies etc.

**Persoonlijk:** dingen over een individu of groep die niet openbaar mogen worden. Als iets persoonlijk is voor iemand, heeft dat meestal betrekking op iets dat als zeer speciaal of gevoelig wordt ervaren.

**Processor:** of 'Central Processing Unit' (CPU) is het deel van de computer dat gegevens verwerkt, controlesignalen verzendt en resultaten opslaat. Samen met het geheugen vormt dit het centrale deel van de computer.

**Proefsoftware:** software die u kunt uitproberen voordat u het echt aankoopt. Proefversies hebben meestal de volledige functionaliteit van de reguliere versie, maar kunnen slechts gedurende een bepaalde periode gebruikt worden.

**Profiel:** persoonlijke gebruikersinformatie in ruimtes voor social networking, instant messaging-systemen, online chattoepassingen, online games etc. Profielen kunnen openbaar of persoonlijk zijn en worden door gebruikers aangepast om zichzelf mee te vertegenwoordigen in virtuele ruimtes.

**Prullenbak:** een directory waarin verwijderde bestanden tijdelijk worden opgeslagen voordat de gebruiker ze definitief verwijdert. U dient regelmatig de oude en ongewenste gegevens uit de prullenbak te verwijderen om ruimte vrij te maken op de harde schijf, het interne geheugen van uw computer.

**P2P-netwerk:** via een 'peer-to-peer' (P2P)-netwerk kunnen degenen die erop aangesloten zijn bestanden uitwisselen door ze te uploaden en te downloaden. Het is slechts één van de diverse manieren waarop bestanden kunnen worden gedeeld op het internet. Bepaalde diensten waarmee bestanden worden gedeeld zijn illegaal.

**Rapportagefunctie:** een functie waarmee gebruikers van openbare virtuele ruimtes een probleem (technisch, onaanvaardbaar gebruikersgedrag, illegale inhoud etc.) kunnen melden aan de moderator of webmaster.

**Ringtone:** een geluid op een mobiele telefoon voor binnenkomende gesprekken. Eigenaars van gsm's kunnen ringtones en muziek downloaden en gebruiken, vaak tegen betaling.

**Scannen:** het met een scanner omzetten van gedrukt materiaal naar digitale bestanden. Hierdoor

kunt u ze als elektronische bestanden bekijken op uw computer en ze online verspreiden.

**Schadelijke inhoud:** foto's, teksten, documenten etc. waarvan de inhoud schadelijk kan zijn. Gewelddadige afbeeldingen zijn bijvoorbeeld ongeschikt en schadelijk voor kinderen en minderjarigen.

**Schermaam:** zie definitie voor Nickname

**Second Life:** de bekende 3D-webgemeenschap van het in de VS gevestigd bedrijf Linden Labs. Gebruikers kunnen virtueel met elkaar in contact komen via een avatar (zie definitie), huizen en diverse omgevingen creëren, handel drijven, virtueel geld verdienen etc. Zie [www.secondlife.com](http://www.secondlife.com)

**SIP-Bench:** een door de Europese Commissie ondersteunde studie waarin de doeltreffendheid getest wordt van de software producten en diensten voor ouderlijke controle en anti-spam die op de Europese markt beschikbaar zijn.

**Social networking:** online gemeenschappen van leden die dezelfde interesses en activiteiten delen en die online met elkaar communiceren via daarvoor geschikte software en diensten (zie social networking sites).

**Social networking sites:** virtuele platforms die gemeenschappen van leden hosten die dezelfde interesses en activiteiten delen. De leden moeten een gebruikersprofiel aanmaken en kunnen teksten, foto's of andere bestanden uploaden, berichten posten en deelnemen aan forums. Veel social networking sites zijn verboden voor kinderen jonger dan 13 jaar en hebben veiligheidsinstellingen voor het profiel.

**Software:** zie definitie voor computerprogramma

**Spam:** ongewenste e-mail, meestal commercieel van aard, met grote hoeveelheden tegelijk verstuurd. Anderen spammen is een van de meest beruchte misbruiken van het internet.

**Spamfilter:** een toepassing die spamberichten blokkeert zodat ze niet in de inbox van uw postvak worden opgeslagen.

**Spyware:** malware die heimelijk aan van het internet gedownloadte bestanden is toegevoegd en zichzelf installeert op de pc en de monitor. Het stuurt de informatie naar een derde partij, vaak bedrijven die geïnteresseerd zijn in het verzamelen van persoonlijke informatie om reclame of andere informatie te sturen, of naar krakers die toegang willen verkrijgen tot persoonlijke gegevens.

**Trojaanse paarden:** kwaadaardige code, malware die uw computer kan binnendringen, verscholen achter ongevaarlijk lijkende zaken zoals games of zelfs programma's die virussen opsporen. Trojaanse paarden vermenigvuldigen zichzelf niet, maar zijn ontworpen om toegang te verkrijgen tot gevoelige informatie of gegevens te vernietigen en kunnen een harde schijf wissen of vertrouwelijke informatie stelen.

**URL ('Uniform Resource Locator');** het adres van een specifieke website of bestand op het internet. Het bevat geen specifieke tekens of spaties en er worden schuine streepjes gebruikt om de verschillende directories aan te duiden. Het eerste deel van het adres geeft aan welk protocol er gebruikt moet worden, het tweede deel specificeert het IP-adres of het domein waar het hulpmiddel is gelocaliseerd.

**Veiligheidsinstellingen (profiel):** een serie van veiligheidsfuncties die u naar uw eigen wensen kan aanpassen en die gekoppeld zijn aan uw online profiel (zie definitie). Deze functies hebben meestal betrekking op het openen van beelden en bestanden, het identificeren van betrouwbare informatieverstrekkers en het vermijden van pornografische inhoud.

**Virtuele bezittingen:** een reeks objecten die elke speler van een spel krijgt toegewezen. Elke speler bezit zijn virtuele objecten via een terminal die de objectenset toont.

**Virus:** een kwaadaardige code, malware, ontworpen om zich te verspreiden door tussenkomst van gebruikers. Meestal verspreidt het zich via e-mailbijlagen, maar ook via geïnfecteerde externe geheugenapparatuur (USB-stick, cd-rom).

**Voice over Internet Protocol (VoIP):** technologie waardoor gebruikers na het downloaden van cliëntsoftware via het internet kunnen praten. De gesprekken kunnen gratis zijn voor bellers die elkaar via dezelfde VoIP-cliënt bellen (bijv. Skype, Voicebuster). Dergelijke software biedt meestal ook faciliteiten om te chatten en om bestanden te delen.

**Wachtwoord:** een geheime reeks tekens waarmee de eigenaar toegang krijgt tot een bestand, computer, account of programma als veiligheidsmaatregel tegen onbevoegde gebruikers (zie hoofdstuk Communiceren).

**Wallpaper:** een patroon, foto of een andere grafische voorstelling die de achtergrond van uw computer- of gsm-scherm vormt.

**Web:** afkorting van 'World Wide Web'. Een verzameling online bestanden geformatteerd in HTML ('HyperText Markup Language') die links naar andere documenten bevatten, evenals naar graphics, audio- en videobestanden. Het web is een onderdeel van het internet.

**Webcam:** een camera die kan uitzenden via het web, in instant messaging, pc-toepassingen voor videoconferenties, chatplatforms etc. Camera's met toegang tot het web bestaan uit een digitale camera die beelden uploadt naar een webserver, ofwel doorlopend, ofwel met regelmatige tussenpozen.

**Website:** een plaats op het 'World Wide Web'. Elke website bevat een homepage, het eerste document dat u ziet als u de site bezoekt. Sites bevatten meestal links naar aanvullende bestanden en sites. Websites zijn het eigendom van en worden beheerd door individuen, bedrijven of organisaties.

**Werkbalk:** een reeks icoontjes of knoppen die deel uitmaken van de interface van een softwareprogramma. Werkbalken dienen als een altijd beschikbare, makkelijk te gebruiken interface voor het vervullen van veelvoorkomende functies.

**Worm:** een speciaal soort virus dat zichzelf vermenigvuldigt en zich zonder tussenkomst van een eigenaar over vele computers kan verspreiden en een netwerk kan beschadigen, enorm veel bandbreedte in beslag kan nemen, een computer kan uitschakelen etc.

**Zoekmachine:** een hulpmiddel om naar informatie op websites te zoeken. De bekendste zijn Google en MSN Search. Zoekmachines hebben geavanceerde voorkeursinstellingen voor gebruikers die interessante veiligheidsinstellingen kunnen bevatten.



## E. Nuttige adressen

### **SAFERINTERNET.BE**

Saferinternet.be is een samenwerking tussen Child Focus en het OIVO. Het project en deze site promoten een veilig en slim gebruik van internet en ICT. Dit Belgische Safer Internet-project maakt deel uit van het Safer Internet Plus-programma van de Europese Commissie. Op [www.saferinternet.be](http://www.saferinternet.be) vindt u info over de risico's van online technologieën: inhoudelijke fiches, dossiers, standpunten, pedagogische fiches, spelletjes, filmpjes, interessante links enzovoort.

### **WWW.WEB4ME.BE**

Een probleem op het internet? Dan is web4me het adres voor jou! Deze website is bedoeld voor jongeren, maar ook ouders en leerkrachten vinden er nuttige informatie: hoe reageren op problemen? Hoe kan je ze voorkomen? Waar kan je terecht?

### **WWW.CLICKSAFE.BE**

[www.clicksafe.be](http://www.clicksafe.be) is een website van Child Focus die kinderen, jongeren, ouders en leerkrachten elk op hun manier heel wat informatie geeft over online veiligheid.

## WWW.GEZINSBOND.BE/VEILIGONLINE

[www.gezinsbond.be/veiligonline](http://www.gezinsbond.be/veiligonline) is een website voor ouders die heel duidelijk uitlegt wat de voordelen van nieuwe media en technologieën zijn en hoe je de risico's zoveel mogelijk kan voorkomen. De site geeft heel veel opvoedingstips en via demofilmmpjes leer je een MSN Messenger-account en een profielpagina op een veilige manier te configureren.

De Nederlandse website 'Mijn kind online' ([www.mijnkindonline.nl](http://www.mijnkindonline.nl)) ondersteunt ouders met internettende kinderen. Achter de site gaat de Stichting Mijn Kind Online schuil, een onafhankelijk kenniscentrum Jeugd en Media. Kijk ook eens op [www.mijnkindonline.weblog.nl](http://www.mijnkindonline.weblog.nl) voor bijna dagelijks aangevuld nieuws over kinderen/jongeren en ICT.

Belgische meldpunten:

- [www.stopchildporno.be](http://www.stopchildporno.be): burgerlijk meldpunt voor kinderpornografie op het internet, beheerd door Child Focus
- [www.cyberhate.be](http://www.cyberhate.be): meldpunt voor discriminerende en racistische inhoud op het internet
- [www.ecops.be](http://www.ecops.be): meldpunt van de Federal Computer Crime Unit van de Federale Politie waarop je elke vorm van internetcriminaliteit kan melden.

## INSAFE

Het Europese netwerk dat het bewustzijn rond e-safety wil vergroten en dat alle ICT-gebruikers aanmoedigt om te genieten van de voordelen van het internet (en ICT in het algemeen), maar zonder de mogelijke risico's en gevaren uit het oog te verliezen:

<http://www.saferinternet.org>



Gesteund door:



*Titel: Veilig internet Gezinspakket* • Tot stand gebracht door Insafe/Liberty Global-UPC in 2008  
Prefix: 9789078209 • Id 51950 • ISBN-NUMMER: 9789078209607 • EAN : 9789078209607

Copyright: dit werk valt onder de Creative Commons Naamsvermelding-Niet-commercieel-Geen Afgeleide werken 3.0 Unported Licentie.  
Bezoek om deze licentie te lezen: <http://creativecommons.org/licenses/by-nc-nd/3.0>