

Zo veilig mogelijk op internet.

Tips op een rijtje(besluiten liggen bij ouders, dit zijn slechts adviezen).

- Praat met de kinderen, zorg voor openheid, ga samen met hen op internet,
- vraag de kinderen te laten zien wat zij doen, laat het ze voordoen,
- kijk mee, zet de pc in de huiskamer
- spreek duidelijke regels en omgangsvormen af
- beperk de tijd dat zij op internet mogen
- **voorkeur ouders: tot 12 jaar een half uur per dag en een uur voor een huiswerkopdracht, boven de 12 jaar een uur voor plezier, twee uur inclusief huiswerk**
- \_zet voor kinderen tot 11 jaar de krowser op de pc zodat zij veilig kunnen surfen
- zeg hen Inlognamen en wachtwoorden geheim te houden,
- laat hen niet reageren op vervelende mails of smsjes, laat hen de berichten bewaren als bewijsmateriaal en laten zien,
- zeg hen nooit privé gegevens te vermelden zoals achternaam, telefoonnummer of adres,
- laat hen weggaan van chat/msn als het niet klopt en verwijder onbekenden
- blokkeer ongewenste personen
- neem een ander telefoonnummer voor mobiel als kinderen lastiggevallen worden.
- De regels voor online gedrag bij de pc hangen zoals: geheim houden persoonlijke gegevens, maximale internettijd, omgangsvormen etc.

t.a.v. gamen

Tips:

- Maak afspraken met de kinderen welke spelletjes er mogen worden gespeeld
- controleer wat er gekocht wordt, PEGI geeft de schadelijkheid van beelden aan
- spreek de tijd af dat zij mogen gamen per dag af of stel een time lock in
- Kijk welk spel zij spelen, laat het hen voordoen en praat erover
- Accepteer gamen niet **alleen** als hobby, dat is te beperkt, stimuleer andere hobby's
- Spreek omgangsvormen af
- Druk kinderen op het hart geen persoonlijke gegevens uit te wisselen met anderen

Uitgebreidere informatie, email adressen en sites vindt u hierna.

**w.w.w.krowser.nl**

De Krowser is een handige kinderbrowser waarmee kinderen van 2 tot 10 jaar veilig kunnen surfen. Het programma geeft alleen toegang tot kind-vriendelijke websites, blokkeert dialoogvensters en hinderlijke popups, en bevat een ingebouwde tijdsklok. Uw kind hoeft nog niet te kunnen lezen, omdat het programma volledig wordt bediend met iconen. [Meer...](#)

[Ouders Online](#), de grootste ouders-community van Nederland, verzorgt de distributie van de Krowser voor particulieren.

Met de Krowser kunt u uw kinderen ook veilig naar YouTube filmpjes laten kijken. Een voorbeeld hiervan vindt u bij de thema's.

De volgende sites zijn als laatste toegevoegd aan de portal:

[Zappflat](#) <sup>tip</sup>

[Frokkie en Lola](#)

[Kind.FM](#)

[Dotje.nl](#)

[Wroet](#)

**Een ouder geeft aan: de pc waar mijn kind op speelt, heeft alleen de krowser om te surfen zodat hij niet te maken krijgt met ongewenste zaken. Heeft hij meer nodig of als hij ouder is dan 12, dan ga ik samen met hem kijken op internet en bespreken wat wel en niet kan en waar hij op moet letten.**

[www.mijnkindonline.nl/hyves](http://www.mijnkindonline.nl/hyves)

## **HYVES**

### **Regels**

Ouders die wel met hun kinderen praten over Hyves, blijken ook veel vaker regels te stellen over gedrag op internet dan ouders die niet praten over Hyves. Bijvoorbeeld over het afschermen van hun profiel, of over wie ze wel of niet mogen toevoegen als vriend. Hoe **belangrijk dit soort regels** zijn, blijkt bijvoorbeeld uit de aanwezigheid van **malafide modellenscouts op Hyves** die erop uit zijn geld te verdienen aan jonge tieners door veel inschrijfgeld te vragen: tieners die niet weten van deze praktijken zijn nog kwetsbaarder als ze geen regels hebben over het omgaan met onbekenden via Hyves.

Bij driekwart van de 8-jarigen gelden huisregels over afscherming, maar ook dat neemt geleidelijk af met de leeftijd. Bij 17-jarigen is het nog maar bij 1 op de 10. Terwijl **het stellen van regels wel degelijk ook bij tieners zin heeft**: als ouders de regel hebben opgelegd om het profiel 'op slot' te zetten, staat bij 70% van de kinderen het profiel ook daadwerkelijk deels of geheel afgeschermd. Als ouders zo'n regel niet hebben opgelegd, is dat maar bij 30% van de kinderen het geval.

### **Gratis brochures voor ouders**

Naast het onderzoek Krabbels & Respect plz? ;- ) brengen Stichting Mijn Kind Online en Digivaardig & Digibewust **twee brochures** over Hyves uit: een voor ouders met **kinderen tot 12 jaar** ('Mijn kind op Hyves') en een voor ouders met **pubers** ('Mijn puber op Hyves'). In de brochures staan tips voor ouders en scholen om kinderen op Hyves te begeleiden. De uitgaven zijn **gratis te downloaden**.

### **Hyves op privé zetten**

1. Meld je aan bij Hyves onder je eigen Hyves-naam.

2. Rechtsboven kies je *Mijn Menu (My Menu)*> kies daar onder *Instellingen (Settings)* voor *Privacy*
3. In het scherm dat dan verschijnt, kun je ofwel voor je hele Hyve-pagina aangeven voor wie het zichtbaar mag zijn (onderin het scherm), ofwel per onderdeel.
4. Links in het scherm kun je ook nog van een aantal andere onderdelen aangeven wie dat mag zien.
5. Vergeet niet al je instellingen op te slaan.
  
6. **Stel je hebt je aangemeld bij iemand zijn Hyves als 'lid' – je kunt binnen Hyves groepjes maken, of 'clubjes' – en je wilt dat weer ongedaan maken. Hoe doe je dat?**
7. Ga naar de Hyves waarbij je aangesloten bent en klik dan links op *Unjoin*. Dit gaat dus op een andere manier dan wanneer je je hebt aangemeld als 'vriend' op iemand z'n vriendenlijst en je wilt dat weer intrekken. Dat kan ook, maar dat gaat weer via *Mijn Menu*. Ga naar *Mijn Menu*. Kies *Vrienden* (zie het plaatje bovenaan dit artikel – klik op het plusje).
  
8. **Praat met uw kind over de privacy-instellingen die Hyves heeft** en bedenk samen hardop waarom je er wel of niet gebruik van zou maken. Het gaat er niet om dat je van tevoren kunt bepalen dat één keuze altijd de beste is, maar dat je kinderen gevoelig maakt voor het nadenken over de gevolgen van de verschillende keuzes.
9. Stel bijvoorbeeld eens de vraag of ze zich kunnen voorstellen **in welke situaties iemand gaat zoeken op jouw naam**. En surf samen eens naar [www.wieowie.nl](http://www.wieowie.nl) of [www.spyderweb.nl](http://www.spyderweb.nl) ontdek wat je allemaal kunt vinden. Het onderwerp 'privacy' en 'welke sporen laat je van jezelf achter op internet' zou regelmatig een onderwerp van gesprek kunnen zijn.

## **BLOKKEREN/VERWIJDEREN ONGEWENST BERICHTEN EN PERSONEN msn/Chat**

[http://help.live.com/help.aspx?mkt=nl-nl&project=WL\\_Messengerv9&querytype=keyword&query=nogol](http://help.live.com/help.aspx?mkt=nl-nl&project=WL_Messengerv9&querytype=keyword&query=nogol)

### **Ongevraagde berichten beperken msn-chat**

Als gebruikers u ongevraagd berichten sturen of uitnodigingen die u als [ongewenste berichten](#) beschouwt, kunt u hen blokkeren en rapporteren als [spammers](#). Als u een gebruiker als spammer rapporteert, verzamelt de Messenger-service deze gegevens en worden er beperkingen gesteld aan de accounts van de spammer. Alle rapporten over spammers blijven vertrouwelijk.

### **Klik om uit te vouwen:**

#### ^ [Contactpersonen blokkeren en aan de blokkeringslijst toevoegen.](#)

- Als u een gebruiker wilt blokkeren vanuit een uitnodigingsdialoogvenster, selecteert u **Weigeren** in en klikt u op **OK**.
- Als u een gebruiker vanuit een gespreksvenster wilt blokkeren, klikt u op het pictogram voor blokkeren  en vervolgens op **Contactpersoon blokkeren**.
- Als u een gebruiker vanuit het hoofdvenster wilt blokkeren, klikt u met de rechtermuisknop op de contactpersoon en op het pictogram voor blokkeren en vervolgens op **Contactpersoon blokkeren**.

#### ∨ [Een gebruiker als spammer rapporteren](#)

### **Opmerkingen**

- Als u niet wilt dat verwijderde contactpersonen u kunnen zien en met u in contact kunnen komen, moet u hen blokkeren.
- Als u geblokkeerde contactpersonen uit de contactpersonenlijst verwijdert, blijven ze geblokkeerd, zelfs als u hen later weer toevoegt.

### **Verwante onderwerpen**

[Een contactpersoon toevoegen, wijzigen, verwijderen of blokkeren](#)

[Informatie over communiceren via andere netwerken voor chat berichten](#)

## **Mijn kind on line.**

- **Maak afspraken over de internet-tijd en houd uw kind daaraan.** De maximale tijd die kinderen op internet mogen besteden, zou je afhankelijk kunnen stellen van het doel waarvoor het medium wordt gebruikt. **Ouder dan 12 jaar** chatten en spelletjes een uur, huiswerk twee uur, zoiets. Als daar een goede reden voor is kunt u natuurlijk best een keer van de algemene regel, maar spreek in ieder geval af dat uw kind op tijd aan tafel komt, op tijd naar bed gaat, en zijn huiswerk niet laat liggen.
- **Help ze heel bewust bij het verdelen van hun tijd:** computer voor school moet eerst, en dan computer voor het eigen plezier. Zit een kind eenmaal op de middelbare school, dan is het belangrijk om ze te helpen bij het plannen van hun tijd. Een puber kan dat meestal niet uit zichzelf. Ze verliezen ook het gevoel van tijd als ze aan het gamen of MSN-en zijn. Vertel ze daarom regelmatig tussendoor hoe laat het is, en vraag naar hun taken voor school.
- **Zorg dat uw kind voldoende pauzes neemt:** eigenlijk ieder uur een pauze van 10 minuten. Tussendoor wat bewegen is nog beter. Let er ook op dat uw kind voldoende tijd aan andere dingen dan computeren besteedt. Zo is het voor jongens heel belangrijk dat ze ontdekken dat ze ook op andere manieren dan bij het gamen, succes kunnen hebben in iets waarvoor ze trainen en waar ze goed in zijn. Let er ook op dat een kind voldoende tijd neemt om normaal te eten en te drinken. Dat vergeet je zomaar als je achter de computer zit...

## PHISHING

Het phishingfilter is een dynamische, nieuwe technologie die u beschermt tegen frauduleuze webpraktijken en het risico van diefstal van persoonlijke gegevens. Phishing is een techniek waarbij iemand probeert om u naar misleidende webpagina's te lokken waar uw persoonlijke informatie en creditcardgegevens kunnen worden verzameld ten behoeve van criminele activiteiten. Deze vorm van identiteitsdiefstal op internet neemt steeds grotere vormen aan.

### Veiligheidsadviezen van de overheid

<http://www.nederlandveilig.nl/veiliginternetten/tips/>

Hier vindt u een aantal veiligheidstips voor als u online gaat met uw kind van 2 tot 10 jaar:

1. U kunt niet vroeg genoeg beginnen met het stimuleren van open en positieve communicatie met kinderen. Het is goed met hen te praten over computers en open te staan voor hun vragen en belangstelling.
2. Op deze leeftijd kunt u het beste samen met hen online gaan.
3. Stel duidelijke regels in voor het gebruik van internet.
4. Hamer er op dat uw kinderen geen persoonlijke gegevens delen met mensen die zij online ontmoeten, zoals hun echte naam, adres, telefoonnummer of wachtwoord.
5. Als op een site naar een naam wordt gevraagd om de inhoud van de site te personaliseren, leg uw kinderen dan uit dat het verstandiger is een bijnaam te gebruiken in plaats van een echte naam, zodat geen persoonlijke informatie wordt vrijgegeven.
6. Vergelijk webfilterhulpprogramma's (zoals **Ouderlijk toezicht van Windows Vista** of **Family Safety van Windows Live** voor Windows XP SP2) voor omgang met uw kinderen en ouderlijk toezicht.

7. Als u beveiligingshulpmiddelen voor gezinnen gebruikt, kunt u de juiste profielen maken voor alle gezinsleden op basis van hun leeftijd. Zie **Family Safety van Windows Live** of **Windows Vista Ouderlijk toezicht** voor meer informatie.
8. Bescherm uw kinderen tegen aanstootgevende pop-upvensters door de pop-upblokkering te gebruiken die in **Internet Explorer** is ingebouwd.

Met Windows Defender kunt u voorkomen dat er pop-upvensters worden weergegeven als u niet met Internet Explorer surft. Windows Defender maakt deel uit van **Windows Vista**. Als u Windows XP SP2 hebt, kunt u **Windows Defender** gratis downloaden.

9. Alle gezinsleden zouden een voorbeeld moeten zijn voor jongere kinderen die pas beginnen met internetgebruik.

#### Veiligheidsadviezen

Hier vindt u een aantal aandachtspunten voor als u online gaat met uw kind van 11 tot 14:

1. Het is altijd raadzaam open en positief met uw kinderen te communiceren. Praat met ze over computers en sta open voor hun vragen en nieuwsgierigheid.
2. Stel duidelijke regels in voor het gebruik van internet.
3. Sta erop dat uw kinderen aan mensen die ze online ontmoeten, geen persoonlijke informatie prijsgeven, zoals hun echte naam, adres, telefoonnummer of wachtwoorden.
4. Als op een site naar een naam wordt gevraagd om de inhoud van de site te personaliseren, leg uw kinderen dan uit dat het verstandiger is bijnamen te gebruiken in plaats van een echte naam, zodat geen persoonlijke informatie wordt vrijgegeven.
5. Gebruik beveiligingshulpmiddelen voor gezinnen om goede profielen te maken voor alle gezinsleden.

Zie **Family Safety van Windows Live** of **Windows Vista Ouderlijk**

**toezicht** voor meer informatie.

6. Stel veiligheidshulpmiddelen in op een "normaal" niveau, zodat er sprake is van enige beperking ten aanzien van inhoud, websites en activiteiten.
7. Plaats computers die met internet zijn verbonden in een open ruimte, zodat u een oogje in het zeil kunt houden als uw kinderen de computer gebruiken.
8. Kijk naar de mogelijkheden van internetfilters (zoals de functie **Family Safety van Windows Live**) als aanvulling op uw eigen toezicht.
9. Bescherm uw kinderen tegen aanstootgevende pop-upvensters door de pop-upblokkering te gebruiken die in **Internet Explorer** is ingebouwd.

Met Windows Defender kunt u voorkomen dat er pop-upvensters worden weergegeven als u niet met Internet Explorer surft. Windows Defender maakt deel uit van **Windows Vista**. Als u Windows XP SP2 hebt, kunt u **Windows Defender** gratis downloaden.

10. Druk uw kinderen daarnaast op het hart dat zij het u komen vertellen als ze zich door iets of iemand op het internet ongemakkelijk of bedreigd voelen. Blijf kalm en druk uw kinderen op het hart dat ze zich niet schuldig hoeven te voelen of bang hoeven te zijn voor straf. Geef ze een compliment omdat ze het hebben verteld en moedig ze aan dat opnieuw te doen als het weer gebeurt.

Meer informatie over hoe u kunt omgaan met **kinderlokken op het web** en **pesten**.

## Kinderlokkers

### Hoe gaan kinderlokkers op het net te werk?

Kinderlokkers leggen contact met kinderen via conversaties in chatrooms, via expresberichten, e-mail of discussieborden. Veel tieners gebruiken onlineforums waarop leeftijdsgenoten elkaar steunen bij het bespreken en oplossen van problemen. Kinderlokkers bezoeken dergelijke ruimten op het web gericht om naar kwetsbare slachtoffers te zoeken.

Kinderlokkers op het web verleiden de personen op wie ze zich richten stap voor stap met aandacht, toewijding, vriendelijkheid en zelfs cadeautjes. Ze besteden hieraan vaak veel tijd, geld en energie. Ze zijn op de hoogte van de nieuwste ontwikkelingen op het gebied van hobby's en muziek die kinderen leuk vinden.

### Hoe kan een ouder voorkomen dat een kind het slachtoffer wordt van dergelijke praktijken?

- Praat met uw kinderen over kinderlokkers en de gevaren van internet.
- Gebruik software voor ouderlijk toezicht, zoals de software die is ingebouwd in **Windows Vista**, of software die u gratis kunt downloaden, zoals de functie **Ouderlijk toezicht van Windows Live**.
- Sta erop dat uw kinderen zich houden aan de leeftijdsgrens van **websites voor sociale contacten**. De adviesleeftijd voor het aanmelden bij een website voor sociale contacten zoals Windows Live Spaces of MySpace is meestal 13 jaar en ouder. Laat uw kinderen deze sites niet gebruiken als ze de adviesleeftijd nog niet hebben bereikt.
- Jonge kinderen moeten geen chatrooms gebruiken omdat de risico's gewoonweg te groot zijn. Kinderen die iets ouder zijn kunt u wijzen op chatrooms voor jongeren die goed worden bewaakt. Zelfs tieners moet u aanmoedigen om chatrooms met bewaking te gebruiken.
- Als uw kinderen chatten in chatrooms, moet u ervoor zorgen dat u weet welke ruimten dat zijn en met wie ze daar praten. Houd de chatrooms in de gaten om na te gaan wat voor soort conversaties er plaatsvinden.
- Leg kinderen uit dat ze het openbare gedeelte van een chatroom nooit moeten verlaten. Veel chatrooms beschikken over privéruimten waar gebruikers onder vier ogen kunnen chatten. Monitors kunnen dergelijke conversaties niet lezen. Dergelijke ruimten worden ook wel fluisterruimten genoemd.
- Zet de computer met de internetverbinding in een gedeelde ruimte van het huis, maar nooit in de kinderkamer. Het is voor een kinderlokker veel moeilijker om een relatie te leggen met uw kind als het computerscherm voortdurend zichtbaar is. Zelfs als de computer in een gedeelde ruimte staat, moet u bij het kind zitten als het op het web surft.
- En als kinderen jong zijn, is het aan te raden om een gezamenlijke e-mailadres te gebruiken en hen nog geen eigen e-mailadres te geven. Als ze ouder worden, kunt u uw internetprovider vragen om een eigen e-mailadres in te stellen voor uw kinderen, maar zorg er wel voor dat het adres zich in uw account bevindt.
- Leg kinderen uit om nooit te reageren op expresberichten of e-mailberichten van vreemden. Als uw kinderen computers gebruiken op een plaats waarop u geen toezicht kunt houden, zoals in de openbare bibliotheek, op school of thuis bij een vriendje of vriendinnetje, moet u nagaan of die computers zijn beveiligd.
- Als uw kind ondanks alle veiligheidsmaatregelen wordt geconfronteerd met een kinderlokker op het web, moet u het kind daarvan nooit de schuld geven. De schuld ligt altijd bij de andere partij. Onderneem actie om te voorkomen dat uw kind nog langer contact heeft met deze persoon.

## Hoe kunnen uw kinderen het risico om slachtoffer te worden zo klein mogelijk maken?

Kinderen kunnen een aantal voorzorgsmaatregelen nemen. Zoals:

- Nooit afbeeldingen downloaden van een onbekende bron; deze kunnen expliciet seksuele inhoud bevatten.
- **E-mailfilters** gebruiken.
- Direct aan een volwassene melden als iets waarmee ze op internet zijn geconfronteerd, hen bang maakt of een onaangenaam gevoel geeft.
- Een schermnaam kiezen die niet naar hun sekse verwijst en geen suggestieve woorden bevat of persoonlijke gegevens prijsgeeft.
- Nooit persoonlijke informatie over zichzelf prijsgeven (waaronder leeftijd en geslacht) of informatie over het gezin aan personen op het web en nooit persoonlijke onlineprofielen invullen. Zie voor meer informatie over specifieke regels over persoonlijke informatie op sites als Windows Live Spaces of MySpace [Uw kinderen helpen veilig om te gaan met websites voor sociale contacten](#).
- Elke e-mailcommunicatie, conversatie via expresberichten of chats direct stoppen als iemand vragen begint te stellen die te persoonlijk zijn of een seksuele lading hebben.
- De overeenkomst binnen het gezin over onlinegedrag bij de computer hangen, zodat ze niet vergeten dat ze hun privacy moeten beschermen.

## Habbo Hotel – Wikipedia

Habbo is voor kinderen van 12 tot 18 jaar.

Om Habbo Hotel te kunnen spelen moet men eerst een Habbo creëren. Een Habbo is een **virtueel karakter** waarmee je rondloopt door het **hotel**. Je moet voor je karakter een naam opgeven en een kleine beschrijving, de zogenaamde *missie*. Deze missie wordt aan andere spelers getoond wanneer er op je karakter wordt geklikt. Je kan ook eigen kleding uitkiezen voor je Habbo, een eigen kapsel uitkiezen en allerlei andere accessoires kopen. Eigenschappen van een Habbo kunnen later worden veranderd. Registratie vindt plaats met een **emailadres**; gebruikers jonger dan 12 jaar moesten daarnaast ook een emailadres van hun ouders invoeren, dit is nadien veranderd en gebruikers jonger dan 12 jaar worden nu niet meer toegestaan in Habbo Hotel.

Meubilair voor de privévertrekken worden uit een catalogus verkregen. Naast meubilair staan er ook andere spullen, zoals huisdieren in de catalogus. Deze zaken kunnen gekocht worden met de zogenoemde *credits*, of geruild worden met andere Habbo's (al kunnen sommige meubels niet geruild worden). Credits moeten via de site gekocht worden met echt geld. Meubels, credits en de privévertrekken kunnen niet van één hotel naar een ander hotel worden overgebracht. Meubilair wordt ook wel "meubi" of "furni" genoemd in het Habbo Hotel. Er kan ook gespaard worden voor meubels door punten te scoren.

Dieven/scammers vragen Habbo's om wachtwoorden om hun meubels te kunnen stelen. Ze zeggen dat als je je wachtwoord geeft dat je dan meubels/credits krijgt, maar dit blijkt achteraf niet waar te zijn.

Ook telefoonfraude komt veel voor. Dieven/scammers maken dan een website die lijkt op een echte Habbo site, en doen alsof ze de baas zijn van Habbo Hotel.

Als er gescholden of bedreigd wordt op Habbo, is een mail aan habbo voldoende om degene die de regels overtreedt, te laten verwijderen.

Email adressen voor informatie met betrekking tot internet gebruik waar naar verwezen wordt tijdens de cyberouder avond.

**[www.mijnkindonline.nl/hyves](http://www.mijnkindonline.nl/hyves)**

onderzoek ouders over hun kind en internet, informatie over hyves etc.

**[www.mijndigitalewereld.nl](http://www.mijndigitalewereld.nl)**

informatie over internetten, veilig gebruik mobiele telefoon etc. heeft veel onderwerpen

**[www.watchyourspace.nl](http://www.watchyourspace.nl)** en **[www.i-respect.nl](http://www.i-respect.nl)**

taalgebruik op internet

**[www.veilig.kennisnet.nl](http://www.veilig.kennisnet.nl)**

over veilig gebruik internet

**[www.pestweb.nl](http://www.pestweb.nl)** en **[www.voo.nl/pesten](http://www.voo.nl/pesten)**

informatie over pesten op internet, mobiele telefoon

**[www.weetwatzegamen.nl](http://www.weetwatzegamen.nl)**

informatie over games op de computer e.a.

