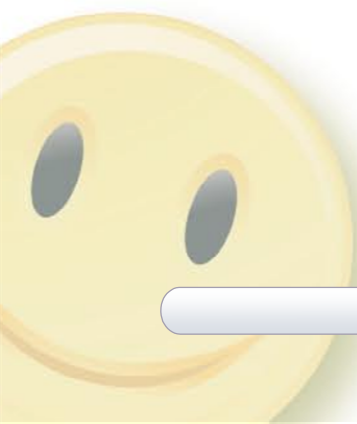




Leerkrachtenhandleiding




Veilig Internet en het intellectueel eigendom

Het lesmateriaal wordt vrijgegeven door middel van een zogenaamde Creative Commons licentie. Er zijn verschillende licenties die de gebruiker verschillende rechten geven. Er is gekozen voor de licentie: Naamsvermelding-NietCommercieel-GeenAfgeleideWerken. Dit betekent dat de gebruiker het werk onbeperkt mag kopiëren, verspreiden, tonen en op- en uitvoeren. Maar de gebruiker mag het werk niet voor commerciële doeleinden gebruiken en de gebruiker mag het werk ook niet bewerken.

Deze uitgave is gebaseerd op de gelijknamige Nederlandse uitgave waarvoor REN Vlaanderen de bewerkingsrechten kreeg via het Nederlandse ministerie van Economische zaken en het Vlaams ministerie van Onderwijs en Vorming.

De Belgische adaptatie is van de hand van Michel Janssens, verbonden aan Xios hogeschool Hasselt.




De voorwaarden staan hieronder vermeld. De volledige tekst van de licentie is te vinden op www.creativecommons.org/licenses/by-nc-nd/2.5/nl/legalcode.


COMMONS DEED

Naamsvermelding-NietCommercieel-GeenAfgeleideWerken 2.5 Nederland

De gebruiker mag:

- het werk kopiëren, verspreiden, tonen en op- en uitvoeren
- Onder de volgende voorwaarden:

Naamsvermelding.
De gebruiker dient bij het werk de door de maker of de licentiegever aangegeven naam te vermelden.

Niet-commercieel.
De gebruiker mag het werk niet voor commerciële doeleinden gebruiken.

Geen Afgeleide werken.
De gebruiker mag het werk niet bewerken.

- Bij hergebruik of verspreiding dient de gebruiker de licentievoorzwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

Het voorgaande laat de wettelijke beperkingen op de intellectuele eigendomsrechten onverlet.

Dit is de vereenvoudigde (human-readable) versie van de volledige licentie.

**Leerkrachtenhandleiding
Secundair onderwijs – 1^{ste} graad**



Stichting Kennisnet Ict op School



Inhoudsopgave

1	Inleiding lespakket veilig internetgebruik	7
1.1	Waarom lessen veilig internetgebruik?	7
1.2	Eindtermen en Veilig internetten	7
1.3	De eindtermen ICT voor het secundair onderwijs	8
1.4	Hoe kinderen veilig laten internetten?	12
1.5	De cursus	14
2	Opzet van de lessen	18
3	Wat heb je nodig om de lessen te geven?	20
3.1	Je (voor)kennis	20
3.2	Leermiddelen	20
3.3	Lesaanpak	20
3.4	De achtergrondinformatie	21
3.5	Groepsgesprekken	21
3.6	Opdrachten	21
3.6	De gebruikte websites	22
4	De lessen en opdrachten Niveau II	24
4.1	Hoofdstuk 1 Ik surf veilig	24
	Hoofdstuk 2 Wat is e-mail?	32
	Hoofdstuk 3 Wie ben jij op internet?	41
	Hoofdstuk 4 Blijf lekker buiten	50
	Hoofdstuk 5 Gewoon doen of niet?	57
	Hoofdstuk 6 Digitaal pesten	63
	Hoofdstuk 7 Lang, langer, langst!	70
	Hoofdstuk 8 Internet is cool	76
5	Knipbladen	Fout! Bladwijzer niet gedefinieerd.
__	Knipblad 1 bij Opdracht 19 ‘ Wat dan’	Fout! Bladwijzer niet gedefinieerd.
__	Knipblad 2 bij Opdracht 19 ‘ Wat dan’	Fout! Bladwijzer niet gedefinieerd.
6	Interessante websites	79
7	Interessante literatuur	82
8	Moeilijke woordenlijst	84

1 Inleiding lespakket veilig internetgebruik

1.1 Waarom lessen veilig internetgebruik?

Leerkrachten in de diverse onderwijsnetten hebben de voorbije jaren heel wat inspanningen geleverd om kinderen te introduceren in de enorme wereld van internet. Dit is namelijk een gigantische bron van een leeromgeving: de leerlingen krijgen toegang tot een immense bibliotheek van alle materiaal, gaande van afbeeldingen van olifanten tot handleidingen voor het maken van bommen. Bovendien gebruiken ze datzelfde internet als communicatieplatform: e-mailen, chatten, nieuwsgroepen, enz. Hiertegenover staat dat leerlingen, meer dan ooit, gevaar lopen dat kinderen op het internet zaken doen die niet voor hen bestemd zijn, of zelfs helemaal illegaal zijn. Regelmatig komen ze in contact met pornosites, racistische taal, ongewenste reclame, pestberichten, enz. Ze hoeven daarvoor zelf niets te doen. De leerlingen krijgen ongewenst allerlei informatie via pop-ups, banners en e-mail.

Nochtans mag dit gevaar geen beletsel vormen om je kinderen te verbieden om op het internet te werken. Educatief gebruik van internet biedt een enorme meerwaarde voor ons onderwijs, en bijgevolg voor elke leerling.

Daarom is het uiterst belangrijk om via het onderwijs het surfgedrag van de kinderen te sturen. Dit kan door hen een kritische houding te laten aannemen ten opzichte van het internet.

1.2 Eindtermen en Veilig internetten

Elke leerling moet overweg kunnen met computer en internet

Persmededeling Kabinet Vlaams minister van Onderwijs en Vorming
datum: 27 oktober 2006

Alle leerlingen in het basisonderwijs en de eerste graad van het secundair moeten leren omgaan met informatie- en communicatietechnologie (ICT). Onderwijsminister Frank Vandenbroucke heeft daarom voor deze niveaus vakoverschrijdende ICT-eindtermen opgesteld, die ingaan op 1 september 2007. In de tweede en derde graad van het secundair onderwijs bestaan al vakgebonden ICT-eindtermen. Nu de eindtermen goedgekeurd zijn door de Vlaamse regering, worden ze voorgelegd aan het Vlaams parlement.

Zoals in de eindtermen (vakoverschrijdende eindtermen Leren leren) vermeld wordt, moeten leerlingen op “informatiebronnen adequaat kunnen raadplegen“ (Bron: www.ond.vlaanderen.be/dvo/secundair/1stegraad/a-stroom/eindtermen/lerenleren.htm). Dat geldt voor de conventionele media zoals de krant en de televisie, maar ook voor het internet. Samen surfen en praten over het internet is de beste manier om kinderen te wapenen tegen de mogelijke gevaren van internet.

Het lespakket “Veilig internet” is te vergelijken met andere cursussen die kinderen in de klas krijgen. Om hun vaardigheden te toetsen hebben we deze lessen bedacht om kennis op te doen en vaardigheden te oefenen, zowel voor de leerling als de leerkracht ...

De vaardigheid om te zwemmen of om deel te nemen aan het verkeer hebben kinderen niet of nauwelijks als ze beginnen met de lessen. Bij internet is dat in de meeste gevallen anders. Je leerlingen internetten vaak al als de besten! Kinderen surfen, chatten, downloaden dat het een lieve lust is. Over internet of computers hoeven wij als opvoeders kinderen vaak niets meer te vertellen... of toch wel? Ja zeker: hier komt het lespakket ‘Veilig internet’ om de hoek kijken. Want natuurlijk surfen en chatten de meeste kinderen, maar weten ze ook hoe ze goed moeten zoeken op internet of hoe ze vervelende zaken kunnen oplossen? Het lespakket ‘Veilig internet’ stelt hen in staat om wél problemen met internet te herkennen en op te lossen of ze tijdig te voorkomen.

1.3 De eindtermen ICT voor het secundair onderwijs

De achtergrond

Er wordt op het vlak van ICT-integratie een nood aan houvast vastgesteld in het basis- en secundair onderwijs. De komst van de ICT-coördinator heeft die vraag nog versterkt. Er bestond tot zeer recent geen bindend referentiekader voor een verantwoorde en educatief zinvolle integratie van ICT in de klaspraktijk. Dat werkt niet enkel een groeiende ongelijkheid in de hand, maar brengt ook onrust en bad-practice met zich mee, zoals:

- onzekerheid over wat kinderen en jongeren wel en niet moeten leren over/met/door de computer;
- veel diversiteit in de aanpak (leren typen, applicatieprogramma's aanleren, een website leren maken,...);

De Vlaamse overheid heeft het ICT-gebruik op verschillende manieren ondersteund, onder meer met geld voor apparatuur, vorming en nascholing en met de professionalisering van het ICT-schoolbeleid via de invoering van de ICT-coördinatoren. Alhoewel de ondersteuning van de ICT-coördinatoren dikwijls als onvoldoende wordt ervaren en de PC/KD-middelen inmiddels werden stopgezet, hebben beide initiatieven onder meer geleid tot een groeiende vraag naar opleiding en/of nascholing over ICT in de lerarenopleiding, bij de begeleiding en de nascholing. Het was echter voor al deze instanties onduidelijk waarop al deze vormingsactiviteiten zich moeten baseren, wanneer zij een coherente visie en daarop geënte inhoud willen aanbieden aan de (aspirant-)leerkrachten. Daarom is bij de regionale expertisecentra ingegaan op de nood om pasklare pakketten te ontwikkelen. 'Veilig internet' is een eerste uitvloeisel hiervan. De leerkracht kan door integratie van deze lespakketten heel wat eindtermen nastreven, zowel voor ICT als voor andere domeinen.

In de loop van 2005-2006 door de DVO (Dienst voor onderwijsontwikkeling) een voorstel van eindtermen en ontwikkelingsdoelen voor ICT uitgewerkt. Deze vakoverschrijdende eindtermen worden ingevoerd op 1 september 2007. De overheid heeft ervoor gekozen om met de eindtermen alleen de contouren aan te geven waarbinnen de school met haar leerlingen aan ICT dient te werken. Ze beklemtoont ook dat het leren omgaan met ICT niet in een apart vak thuishoort, zoals dat bijvoorbeeld voor informatica het geval is.

De interpretatie van de eindtermen

De eindtermen zijn breed geformuleerd als competenties en attitudes, en ze hebben het statuut van leergebiedoverschrijdende eindtermen. Ze zijn dermate algemeen geformuleerd, dat er voor de toepassing in de onderwijspraktijk nog enkele bewerkingen wenselijk zijn.

In de eerste plaats dient werk gemaakt van de specificering van de ICT-doelen. Dat betekent dat elke ICT-competentie in meer elementaire doelen of tussendoelen wordt vertaald. In die specifieke doelen worden bepaalde kenniselementen genoemd, wordt naar specifieke applicaties verwezen en wordt het beheersingsniveau aangegeven (beogen we bijvoorbeeld opvolgen van een gesloten opdracht, of beogen we ook zelf een vorm van verwerking kunnen kiezen?).

Ten tweede kunnen die specifieke doelen (per eindterm of ICT-competentie) geordend worden naar de volgorde waarin ze doorheen de leerjaren van het (basis)onderwijs best aan bod komen. Men kan ze met andere woorden op een leerlijn plaatsen. Het is nochtans aan te raden om de leerlingen zo snel mogelijk wegwijs te maken in veilig internetten. Over deze basisvaardigheid moeten de leerlingen beschikken vooraleer ze andere doelen, zoals efficiënt informatie verzamelen, nastreven.

Enkele uitgangspunten

Een van de uitgangspunten bij het opstellen van de eindtermen ICT is het **maatschappelijke draagvlak**. Vanuit verschillende kanalen in de samenleving wordt aan het onderwijs gevraagd om rekening te houden met de mogelijkheden van ICT in het onderwijs. De samenleving evolueert naar een kennissamenleving waarin het omgaan met ICT een belangrijke basiscompetentie is geworden. Naarmate ICT meer geïntegreerd raakt in de maatschappij, wordt het kunnen gebruiken van ICT steeds meer een voorwaarde voor zelfstandig functioneren. Onderwijs zal dus aandacht moeten besteden aan kennis, inzichten, vaardigheden en attitudes rond ICT. De maatschappelijke context vraagt een specifieke invulling van de ICT-competentie. Wat nodig is, is het probleemoplossend vermogen om met behulp van ICT taken, problemen, aspiraties adequaat aan te pakken. Dat is een complexe competentie die ver afstaat van het aanreiken van één-op-één-oplossingen of het aanleren van louter technische, instrumentele of procedurele vaardigheden. Veilig internetten zal veel meer moeten zijn dan het louter aanreiken van enkele 'tools' om veilig te surfen en/of e-mailen. Er zal in de klas een gesprek moeten plaatsvinden over een veel breder spectrum, gaande van (digitaal) pesten (op school) tot verantwoord communiceren (via chatboxen), enz.

Bovendien moet de formulering van de eindtermen rekening houden met de **buitenschoolse context**. Ook heeft het onderwijs de verantwoordelijkheid om leerlingen op een veilige, bewuste en kritische manier te leren omgaan met ICT, een vaardigheid die jongeren doorgaans niet spontaan verwerven in een buitenschoolse context. Vooral **veilig internetgebruik** blijkt een groeiend knelpunt voor jonge kinderen. Onderzoek maakt duidelijk dat de meeste jongeren in hun vrije tijd meer ICT-vaardigheden verwerven dan op school. De school moet hiermee rekening houden en hierop verder bouwen. Daarbij moet ze bijzondere aandacht schenken aan vaardigheden die minder snel verworven worden buiten de school. In tegenstelling tot het inductieve leren thuis, zou dat binnen het onderwijs kunnen leiden tot graduele cursussen over instrumenteel ICT-leren. De overtuiging groeit echter in binnen- en buitenland dat het verwerven van technische vaardigheden voor het basisonderwijs en de eerste graad van het secundair onderwijs ondergeschikt zijn aan het verwerven van betere informatie-, expressie- en communicatievaardigheden, die wel van cruciaal belang blijken voor (levenslang) lerenden.

Integratie ICT

Eindtermen/ontwikkelingsdoelen voor ICT schetsen de contouren van wat van de school wordt verwacht op vlak van ICT. Dit zorgt geenszins voor een uniformisering van wat er in scholen zal gebeuren met ICT. Door de keuze voor leergebied-/vakoverschrijdende eindtermen is het nadrukkelijk niet de bedoeling om er een apart vak van te maken. ICT biedt kansen binnen alle vakken en leergebieden. Evenwel doen de eindtermen/ontwikkelingsdoelen geen uitspraak hoe en in welke vakken of leergebieden ICT moet worden geïntegreerd. Het is aan de school om daar afspraken rond te maken. Op het eerste gezicht is deze cursus ontwikkeld om 'binnen' ICT te behandelen, maar als leerkracht kan je deze onderwerpen kaderen in een groter geheel. Zo kan je het deel over 'gezondheid en RSI' kaderen in een vakoverschrijdend domein rond lichaam, gezondheid, enz. Netiquette past perfect in een werkstuk rond Nederlands, verantwoord communiceren, enz.

Versillende studies in het buitenland tonen aan dat de integratiegraad van ICT in de klas, ondanks alle overheidsmaatregelen, behoorlijk laag ligt. Zolang er in scholen weinig leertijd wordt uitgetrokken om met ICT te leren omgaan, of via ICT kennis en vaardigheden te verwerven, kan men ook niet verwachten dat ICT een effect heeft op het leerrendement. Een van de eerste dingen die een leerling, maar ook leerkracht, moet leren is omgaan met de mogelijke gevaren van het internet. De leerkracht moet dit thema bespreekbaar maken in de klas.

Toelichting bij de ICT -eindtermen en ontwikkelingsdoelen voor het secundair onderwijs

Secundair onderwijs, eerste graad A-stroom: vakoverschrijdende eindtermen ICT

eindtermen en ontwikkelingsdoelen secundair: [eerste graad](#) - [tweede graad](#) - [derde graad](#)
(Ga naar uitgangspunten)

Voor het secundair onderwijs A- en B-stroom, en BUSO OV3

De leerlingen

- 1 hebben een positieve houding tegenover ICT en zijn bereid ICT te gebruiken om hen te ondersteunen bij het leren.
- 2 gebruiken ICT op een veilige, verantwoorde en doelmatige manier.
- 3 kunnen zelfstandig oefenen in een door ICT ondersteunde leeromgeving.
- 4 kunnen zelfstandig leren in een door ICT ondersteunde leeromgeving.
- 5 kunnen ICT gebruiken om eigen ideeën creatief vorm te geven.
- 6 kunnen met behulp van ICT digitale informatie opzoeken, verwerken en bewaren.
- 7 kunnen ICT gebruiken bij het voorstellen van informatie aan anderen.
- 8 kunnen ICT gebruiken om op een veilige, verantwoorde en doelmatige manier te communiceren.
- 9 kunnen afhankelijk van het te bereiken doel adequaat kiezen uit verschillende ICT-toepassingen.
- 10 zijn bereid hun handelen bij te sturen na reflectie over hun eigen en elkaars ICT-gebruik.

Deze cursus wil vooral inspelen op eindtermen/ontwikkelingsdoelen 2, nl. 'veilig internet', 8 'veilig communiceren' en 10 'reflecteren'.

Eindterm/ontwikkelingsdoel 2: De leerlingen gebruiken ICT op een veilige, verantwoorde en doelmatige manier.

- Met 'veilig' wordt bedoeld dat leerlingen alert zijn voor ondermeer schadelijke of discriminerende inhoud en voor het bestaan van virussen, spam en pop-ups. Ze geven geen persoonlijke en vertrouwelijke informatie door aan onbekenden. Ze kweken de reflex aan om dubieuze berichten en ongewone inhoud te signaleren.
- Bij 'verantwoord gebruik' wordt bijvoorbeeld gedacht aan de zorg voor apparatuur en software. Dat houdt ondermeer in dat leerlingen rekening houden met de financiële en ecologische aspecten van ICT-gebruik: zij printen bv. niet elk document uit en respecteren de afspraken over downloaden en kopiëren. *Verantwoord* gebruik heeft ook ethisch-sociale aspecten. Leerlingen gebruiken ICT niet om anderen lastig te vallen en te pesten. Ze hebben respect voor de intellectuele eigendom van anderen bij het gebruik van informatie en software. Er is ook de zorg voor zichzelf: de leerlingen werken op een ergonomisch verantwoorde manier met de computer.
- 'Doelmatigheid' heeft te maken met zich afvragen of de middelen in verhouding staan tot het doel. Leerlingen leren hun ICT-gebruik kritisch te overdenken. Zij houden bij het werken met ICT steeds hun doel voor ogen. Ze gebruiken ICT enkel waar dat zinvol is, ze proberen bv. de duur van hun ICT-gebruik realistisch in te schatten en te bewaken.

Eindterm/ontwikkelingsdoel 8: De leerlingen kunnen ICT gebruiken om op een veilige, verantwoorde en doelmatige manier te communiceren.

- Met communiceren bedoelen wij hier dat leerlingen de faciliteiten die ICT biedt, kunnen gebruiken om informatie (onder de vorm van woord, beeld, klank) te geven of te vragen aan derden. Daarbij denken wij aan mogelijkheden die een bijdrage kunnen leveren aan het leerproces, zoals afspraken maken via e-mail of SMS, elektronische documenten meesturen met een e-mailbericht, contacten leggen en informatie verzamelen voor een studiebezoek, live chatten met leerlingen van een andere school, gebruiken van internetfora, blogging, enz.
- De toevoegingen 'veilig, verantwoord', focussen op de elementaire regels en omgangsvormen voor ICT-communicatie. De leerlingen leren onder meer omgaan met de conventies en regels die op het net gelden, soms netetiquette genoemd.

- Met 'doelmatig' wordt bedoeld dat leerlingen zich afvragen wat het beste communicatiemiddel is, in functie van hun doel. Het is aan de scholen om te oordelen welke de meest gangbare communicatiemiddelen en - applicaties zijn (of worden in de toekomst).
- Ook voor leerlingen met een verstandelijke beperking bestaan er specifieke ICT-hulpmiddelen voor communicatie.

Eindterm/ ontwikkelingsdoel 10: De leerlingen zijn bereid hun handelen bij te sturen na reflectie over het eigen en elkaars ICT-gebruik.

- Het reflecteren is een gevolg van adequaat leren kiezen. Door te reflecteren op de gebruikte middelen, en de bekomen resultaten te vergelijken, leren de leerlingen de verschillende eigenschappen, voor- en nadelen van de aangewende middelen, programma's, applicaties. Daarom is dit ook een ICT-competentie.
- Het is dus nuttig om leerlingen, probleemoplossend, met verschillende middelen te laten experimenteren. Daarna kunnen de producten en de processen met elkaar vergeleken worden. Deze werkwijze zal hen ervaring opleveren waarvan ze bij een volgende opdracht profijt kunnen halen.

En de andere eindtermen?

ICT is geen losstaand element in het secundair onderwijs. Aan de hand ervan kan gewerkt worden aan heel wat nieuwe eindtermen.

Hier een overzicht. Ze staan per leergebied en domein en de nummering verwijst naar het nummer van de eindterm zelf:

Gezondheidseducatie

- 13 De leerlingen kunnen een goede sta-, zit-, en tilhouding demonstreren en voorbeelden geven van mogelijke klachten die optreden bij verkeerde houdingen en bewegingen.
- 14 De leerlingen zien het belang in van een evenwichtige tijdsbesteding van (school-)werk, rust, ontspanning, beweging en de invloed ervan op de lichaamsconditie.

Leren Leren

- 7 De leerlingen kunnen informatiebronnen adequaat raadplegen:
 - inhoudstafel en register gebruiken;
 - elementen uit audiovisuele en geschreven media gebruiken;
- 11 De leerlingen zijn bereid zelf naar oplossingen te zoeken en durven leer- en studieproblemen signaleren en uitleg of hulp vragen.
- 12 zijn bereid ordelijk, systematisch en regelmatig te werken.
- 13 beseffen dat leren reeds in de klas begint en niet alleen thuis gebeurt.

Opvoeden tot burgerzin

- 1 De leerlingen kunnen aan de hand van het schoolreglement hun rechten en plichten concreet illustreren.
- 2 De leerlingen kennen de functies en verantwoordelijkheden van al wie bij de school betrokken is en kunnen gebruik maken van de middelen die er bestaan om hun vragen, problemen, ideeën of meningen kenbaar te maken.
- 3 De leerlingen kunnen op een verdraagzame manier omgaan met verschillen in sexe, huidskleur en etniciteit.
- 4 De leerlingen kunnen voor conflicten in de omgang met leeftijdgenoten oplossingen bedenken en zijn bereid om ze uit te voeren.
- 9 De leerlingen kunnen de invloed van de media op hun eigen denken en handelen illustreren en kennen de mogelijkheden van het gebruik ervan ten voordele van de eigen vorming.
- 10 De leerlingen kunnen een kritische houding aannemen ten aanzien van allerlei vormen van berichtgeving.

Sociale vaardigheden

- 2 De leerlingen kunnen respect en waardering opbrengen voor anderen: de

- eigenheid van medeleerlingen accepteren en waarderen.
- 4 De leerlingen kunnen om hulp vragen en dankbaarheid tonen in probleemsituaties.
 - 5 De leerlingen kunnen in groepsverband meewerken en een toegewezen opdracht uitvoeren.
 - 6 De leerlingen kunnen bij een opgegeven groepstaak of bij een groepsdiscussie leiding geven.
 - 7 De leerlingen kunnen op gepaste wijze kritiek uiten tegenover een ander tijdens een groepswerk.
 - 8 De leerlingen kunnen opkomen voor de eigen rechten en voor de rechten van anderen uit de groep.
 - 9 De leerlingen kunnen zich discreet opstellen in een gezelschap en ten aanzien van vertrouwelijke informatie.
 - 12 De leerlingen beheersen elementen van het communicatieve handelen:
 - actief luisteren en weergeven wat een andere inbrengt
 - toegankelijk zijn en feed-back geven over eigen gevoel
 - verduidelijken waarom zij voor een bepaald gedrag gekozen hebben
 - assertief zijn en opkomen voor de rol die zij op zich nemen in een groepsopdracht
 - effectbesef hebben en over hun eigen gedrag reflecteren
 - anderen de kans geven om te reageren
 - 13 De leerlingen leggen contact met anderen binnen de groep en staan open voor contact met anderen buiten de groep.
 - 14 De leerlingen kunnen in een groepsdiscussie hun mening weergeven, handhaven en bijsturen.

1.4 Hoe kinderen veilig laten internetten?

Als school of individuele leerkracht kan je op twee manieren de kinderen beveiligen tegen ondoelmatig gebruik van internet, nl. de technische en de pedagogische aanpak.

De technische aanpak

Als je school een extra vorm van toezicht noodzakelijk vindt, kan ze gebruik maken van de mogelijkheden van het besturingssysteem (Windows, Linux, ...) om controle uit te oefenen:

- men kan gebruik maken van een persoonlijke gebruikersnaam (login) voor elke leerling. Dit systeem van monitoring stelt leerkrachten in staat om controle uit te oefenen op het surf- en mailgedrag van de leerling. Hiermee kan je niet vermijden dat leerlingen ongewild sites bezoeken die niet voor hen bestemd zijn.
- je kan filters gebruiken om de inhoud te beveiligen. In de meeste zoekrobots (Google, Altavista, enz.) staat er standaard een familiefilter aangevinkt om ongewenste inhoud (geweld, sex) tegen te houden. Maar ook dit biedt maar een gedeeltelijke beveiliging, vermits de filter gemakkelijk kan worden omzeild. Sommige providers (verschaffers van internet) bieden wel abonnementen aan voor een schone versie van internet.

Een geïntegreerde aanpak: technologie en opvoedkunde

Een overleg- en praatcultuur heeft vaak meer effect dan technologische snuffjes. Zelfs in de VS lijkt men dat te beseffen. De National Research Council gebruikt een treffend beeld als argument voor een geïntegreerde aanpak waarin opvoeding en technologische vaardigheden mekaar aanvullen. Als je een zwembad hebt en je bent bang dat je kinderen zouden verdrinken, kan je van alles en nog wat ondernemen: sloten installeren, afsluitingen optrekken, speciale bewegingsdetectoren opstellen enzovoort. Om te vermijden dat je kind verdrinkt, kan je het evenwel best leren zwemmen. Dit betekent niet dat de verschillende hulpmiddelen overbodig zijn. Het Departement Onderwijs pleit in de eerste plaats voor een surfcultuur van participatie en overleg,

maar een stok achter de deur kan handig zijn. Afhankelijk van de leeftijd van kinderen is een geïntegreerde aanpak waarin technologische hulpmiddelen en opvoedende maatregelen gecombineerd worden, de beste remedie.

Deze opvoedkundige, technische en beleidsmatige tips kunnen je helpen om als leerkracht, ICT-coördinator of directeur een ICT-beleid uit te bouwen dat veilig internetten op school stimuleert.

Enkele pedagogische tips

- Hou het surfgedrag van je klas in het oog, al dan niet via monitoring. Of je de controle nu uitvoert of niet: als leraar doe je er best aan de leerlingen duidelijk te maken dat je hun surfgedrag kán nakijken.
- Geef jongeren verantwoordelijkheid. Leer hoe ze zelf op het internet kunnen zoeken zonder al te groot risico op ongeoorloofd materiaal.
- Als leraar kan je het gebrek aan objectiviteit en betrouwbaarheid van het internet aankaarten in de les. Enkele voorbeeldtips:
 - o laat de leerlingen op het internet zelf foute berichtgeving en tendentieuze informatie ontmaskeren;
 - o laat hen de voordelen van het internet (bijvoorbeeld de snelheid van het medium, de communicatiemogelijkheden, het democratische gehalte, ...) afwegen tegen de nadelen (politieke propaganda, racisme, agressieve reclame, religieuze indoctrinatie, schending van de privacy);
 - o geef een les over haatsites en de racistische symbolen die op het internet verspreid worden.
- Spreek erover met je leerlingen als je merkt dat ze ongeoorloofde websites bezoeken. Leg uit waarom je niet wil dat je leerlingen bepaalde sites bezoeken. Gaat het om commerciële of andere uitbuiting? Welk beeld van een kind wordt er opgehangen?
- Geef jonge kinderen vertrouwen en stel ze gerust. Als ze toch in aanraking komen met ongewenst materiaal is ons advies: reageer en wees niet bang om erover te praten. Een gesprek over de eigenaardige vondsten op het internet en wat het kind daarbij voelt, is daarbij de beste aanpak.
- In dialoog treden is trouwens ook de beste aanpak bij gewelddadige computerspelletjes: geef je mening als je bepaalde schiet- en vermorzelspelletjes te agressief vindt. Je kan op verschillende manieren op de hoogte blijven van wat er op de markt is: je kan de demo's bekijken in de computerwinkel, in tijdschriften en op het internet. Wie goed op de hoogte blijft, kan kinderen alternatieve spelletjes voorstellen die geen excessief of gruwelijk geweld bevatten. Er zijn door het Departement onderwijs enkele interessante brochures uitgegeven met tal van educatieve spelletjes en andere software (www.ond.vlaanderen.be/publicaties):
 - o ICT, spingplank voor de kleuterklas
 - o ICT op het menu: 65 recepten voor computergebruik in de basisschool
 - o ICT-competenties in het basisonderwijs
 - o Digitale leermiddelen voor het secundair onderwijs

Enkele technische tips

- Directies en ICT-coördinatoren die opteren voor “monitoring” kunnen leerkrachten bijbrengen hoe ze de map geschiedenis in de navigator kunnen openmaken.
- Gebruik eventueel filters. Twee vragen zijn belangrijk bij de keuze voor de juiste software: welke filtermethode gebruikt het programma en is de Nederlandstalige vertaling van de oorspronkelijke trefwoorden goed? Voor ons taalgebied is de

evaluatie van Test-Aankoop toonaangevend. De consumentenorganisatie legde 18 “elektronische babysitters” op de rooster. Slechts drie daarvan bleken doeltreffend: Internet Guard Dog 3.13 van McAfee, N2H2 For Home 1.0 van de gelijknamige firma en We-Blocker 2.0.1 van We-Webcorp. Clickx Magazine beveelt een programma aan dat niet in de studie van Test-Aankoop is opgenomen: Norton Internet Security 2002. Childfocus beveelt nog twee andere filters aan op haar website: Neox en ICRA-filter.

1.5 De cursus

Drie niveaus

Het lesmateriaal van het lespakket ‘Veilig internet’ is geschreven op drie niveaus.

- *Niveau I = tweede graad basisonderwijs*
- *Niveau II = derde graad basisonderwijs*
- *Niveau III = eerste graad secundair onderwijs*

Het verschil zit in het gebruik van termen, de aanspreekwijze van de leerlingen en het niveau van de oefeningen. De verschillende niveaus bevatten dezelfde thema’s, maar kunnen verschillende opdrachten bevatten. Bovendien leiden de niveaus tot dezelfde vaardigheden, zij het dan op verschillende niveaus.

De inhoud van de lessen richt zich op de volgende thema’s:

Een zo veilig mogelijk gebruik van:

- e-mailen, surfen
- chatten / msn-en / profielen
- gebruik maken van de computer zelf

Specifieke thema’s die zijn doorgenomen zijn:

- ongewenste sites
- privacy en privé-gegevens digitaal
- gepest worden virussen (en hackers)
- rsi en verslaving
- regels internetgebruik op school
- Kids-ID

Introductie karakters

Muzaffer, Tine, Jonas en Laura zijn de hoofdfiguren in de lessen. De vier kinderen maken van alles mee op internet en hebben daarbij regelmatig de hulp nodig van elkaar of van de leerlingen.

Muzaffer

Muzaffer is de jongste van het stel. Hij heeft nog niet zoveel op met internet en speelt liever buiten. Als hij eens iets probeert, een leuk spelletje spelen bijvoorbeeld, dan gaat het nog mis ook.

Muzaffer wordt door de andere drie hoofdfiguren geholpen. Muzaffer is daarnaast een positief voorbeeld van een jongen die graag buiten wil spelen.

Tine

Tine is een spring in het veld. Ze duikt overal in en denkt dan niet altijd even goed na over wat ze doet. Daardoor komt ze in de problemen. In het introductiestukje voor de leerlingen geeft ze bijvoorbeeld zomaar haar wachtwoord prijs en heeft ze een bijnaam die op internet misschien heel verkeerde associaties kan oproepen.

Jonas

Jonas is de Whizzkid. Hij weet alles van internet, tenminste, dat denkt hij! Hij is stoer, maar valt ook door de mand. Hij blijkt niet alles te weten. Jonas is degene die veel te vaak met computers en internet bezig is. Zoveel dat de andere drie hoofdfiguren er genoeg van krijgen en hem niet eens meer vragen om met hen mee te doen.

Laura

Laura is verlegen. Ze wil een heleboel doen op internet, maar is een beetje huiverig om van alles uit te proberen. In haar introductietekst in het lesboek geeft ze aan dat ze ooit eens iets besteld blijkt te hebben via internet. Dat was niet haar bedoeling. Ze durft in ieder geval wel hulp te vragen aan de andere drie als ze er niet uitkomt.

In de introductieteksten van de hoofdfiguren in het lesboek wordt een aantal risico's benoemd. Deze risico's komen later in de lessen terug. De leerlingen zullen in diverse lessen de introductieteksten nog een keer lezen om ze te gebruiken tijdens de opdrachten.

De rol van de leerkracht

Het is goed om als leerkracht open te staan voor de verhalen en ervaringen van de leerlingen. Het lijkt alsof kinderen de volwassenen eruit gesurft hebben, maar is dat wel zo? Tenslotte heb je als volwassene al de nodige levenservaring, die de kinderen niet hebben. **Het is dan ook niet belangrijk dat je net zo snel als de leerlingen je weg doorklikt op internet.** Weten wat er speelt op internet en wat kinderen ervaren is wel belangrijk. Er wordt van jou niet verwacht dat je een computerexpert bent! Vergelijk het met een rage. Je hoeft niet precies te weten hoe de puntenstructuur van ruilkaarten in elkaar zit. Je weet van de rage en je weet wat een rage doet met kinderen. Dat is van belang!

Je zal merken dat het onderwerp internet veel los kan maken bij de leerlingen. Wanneer je zelf aangeeft ook ervaring te hebben met internet, weet wat MSN is (en dit vooral niet afdoen met onzin), weet wat chatsites zijn en op de hoogte bent dat er digitaal gepest wordt, dan zal je merken dat de verhalen losbranden. Kinderen hebben vaak het idee dat ze hun ouders en leerkrachten weinig kunnen vertellen over wat ze meemaken op internet, omdat de volwassenen hen toch niet zullen begrijpen. Uit diverse onderzoeken is duidelijk geworden dat kinderen die heel open kunnen praten met hun ouders en/of leerkrachten minder in de problemen komen dan kinderen die dat niet kunnen.

Start het gesprek altijd met het belichten van de leuke kanten van internet. Wat vinden de leerlingen het leukste en waarom? Wat zijn hun favoriete websites en waarom? Pas daarna ga je praten over de risico's van internet. Laat de leerlingen zelf hun ervaringen vertellen, maar vooral ook de oplossingen die ze bedacht hebben. Dit kan je bij elk hoofdstuk herhalen. Dus: positieve kanten van het onderwerp van het hoofdstuk, de risico's, de oplossingen.

Je rol als leerkracht is begeleidend en ondersteunend. Het is van groot belang open te staan voor de verhalen van je leerlingen en hen te leren omgaan met de risico's die internet met zich meebrengt.

De rol van de leerling

De acht hoofdstukken (ongeveer acht lessen) sluiten aan bij de leefwereld van kinderen op internet. Je zal merken dat je leerlingen graag willen vertellen over wat hen bezighoudt. Geef leerlingen de ruimte om over hun eigen ervaringen te vertellen. Waarschijnlijk sta je versteld over wat ze allemaal al weten, tegen zijn gekomen en de oplossingen die ze zelf gevonden hebben. Samen met je leerlingen doorloop je het lesboek en de opdrachten.

De lessen zijn erop gericht om de leerlingen inzicht en vaardigheden aan te leren om op een goede manier om te gaan met internet en de risico's die daarbij horen.

De rol van de ouders

De rol van ouders is van groot belang voor het onderwerp. Kinderen maken namelijk het meeste gebruik van internet in de thuissituatie. Het is belangrijk dat leerlingen niet alleen met hun leerkracht kunnen praten over wat hen bezighoudt op internet, maar zeker ook met hun ouders. Kinderen die thuis in een open sfeer kunnen vertellen wat ze meemaken op internet blijken veel minder in de problemen te komen dan kinderen bij wie dat thuis niet mogelijk is.

Om ouders op de hoogte te stellen van de cursus 'Veilig Internet' kan je hen een brief geven, waarin beknopt staat aangegeven wat de lessen inhouden.

Het is aan te bevelen ouders te betrekken bij de lessen. Wellicht kan je als leerkracht de hulp van ouders gebruiken bij het uitvoeren van de lessen. Zo kan je binnen je school de ouderparticipatie een nieuwe, digitale, invulling geven.

Speciaal voor ouders worden door diverse organisaties voorlichtingsavonden over veilig internet georganiseerd. Je kan tijdens de uitvoering van de lessen voor de leerlingen de ouders extra betrekken door een voorlichtingsavond aan te bieden. Er zijn diverse organisaties die deze voorlichtingsavonden aanbieden:

- www.actioninnocense.org
- www.degezinsbond.be
- www.nedbel.be (de "federal computer crime unit" van de federale politie)

"De gevaren van internet - verantwoord omgaan met internet"



"On the Internet, nobody knows you're a dog."

Op **donderdag 8 maart** om **20 uur** in de **feestzaal** (vestiging **Weggevoerdenstraat**) wordt er, door de Federal Computer Crime Unit (Federale Politie) in samenwerking met het Departement Onderwijs, een uiteenzetting gegeven onder de titel "De gevaren van internet - verantwoord omgaan met internet".

- ♦ *Hoe kunnen we het kaf van het koren onderscheiden?*
- ♦ *Hoe kunnen we zorgen voor een 'veilig' internet voor onze chattende kroost?*
- ♦ *Hoe kunnen we onze jongeren behoeden om niet in de ban te geraken van louche sites of onbetrouwbare contactpersonen?*

Deze en andere vragen zullen aan bod komen tijdens deze avond.






-Jeugdcultuur in de bibliotheek, Antwerpen - 30 januari

VVBAD organiseert op 30 januari 2007 een studiedag in de Antwerpse Pemekebibliotheek over jeugdcultuur. Welke plek krijgen kinderen in een publieke onderneming zoals de bibliotheek? Rita Baptiste, oprichter van HetVanKinderenmuseum (Nederland), ontwikkelde een visie over wat kindercultuur nu eigenlijk is en hoe wij die kunnen terugvinden in de bibliotheek van de toekomst.

Aangezien chatten, gamen en googlen deel uitmaken van de jeugdcultuur, willen we kinderen en jongeren ook beschermen tegen de gevaren ervan. Action Innocence is een ngo die streeft naar een veilig internet. Kim Loots, psychologe bij Action Innocence, geeft preventieworkshops over veilig surfen op het internet. Ze informeert ons over het begeleiden van kinderen en jongeren bij het surfen.

Ouderraad VITO

Mededelingen: B

 Nieuw item |  Item bewerken |  Item verwijderen |  Waarschuw mij |  Terug naar de lijst

Volgorde (letter): B

GemaaktOp: 8-3-2007

Mededeling: >> **INFO-AVOND VEILIG INTERNET**

Op donderdag 26 april 2007 wordt er door de ouderraad van VITO een info-avond georganiseerd omtrent "Veilig internetten".

Het doelpubliek is de ouders van de leerlingen van de eerste graad, maar iedereen is van harte welkom en het is gratis! De leerlingen van de eerste graad krijgen hierover tijdig een brief mee.

2 Opzet van de lessen

De acht hoofdstukken in het lesboek worden gemiddeld in tien lessen van 50 minuten behandeld. Het hangt af van:

- de duur van groepsgesprekken;
- het aantal beschikbare pc's voor de opdrachten;
- het niveau van uitdieping (extra opdrachten in het werkboek).

In hoofdstuk 4 van deze handleiding worden de opdrachten bij de lessen beschreven.

Hoofdstuk 1 Ik surf veilig

Eén van de favoriete bezigheden van je leerlingen is vast en zeker het surfen naar allerlei websites op internet. In dit hoofdstuk komt het gericht zoeken op internet aan bod en de vraag of alles wat op internet staat echt waar is.

Hoofdstuk 2 Wat is e-mail?

Je leerlingen gebruiken e-mail om anderen een berichtje te sturen en ontvangen zelf ook e-mail. In dit hoofdstuk wordt behandeld wat er naast een leuke e-mail nog meer de digitale brievenbus binnenkomt. Daarnaast wordt stilgestaan bij het belang van een goed wachtwoord.

Hoofdstuk 3 Wie ben jij op internet?

Kinderen zijn heel naïef als het gaat om het prijsgeven van privé-gegevens. In dit hoofdstuk wordt behandeld wat privé-gegevens eigenlijk zijn en hoe je daar het beste op internet mee om kunt gaan. Daarnaast komt aan de orde hoe mensen zich voordoen op internet. Hier komt ook de Kids-ID ter sprake.

Hoofdstuk 4 Blijf lekker buiten

Een virus kan de computer kapot maken. Een virus kan overal in zitten, bijvoorbeeld in een e-mailtje. De leerlingen zullen aan de hand van een chemieproefje ondervinden hoe een virus zich kan verspreiden. Andere onderwerpen die aan bod komen zijn spionnen op de computer (spyware). Wat kun je tegen virussen en spyware doen en hoe kun je erop letten dat ze niet achtergelaten worden op de computer?

Hoofdstuk 5 Gewoon doen of niet?

Op veel websites staat reclame. Bijvoorbeeld banners, pop-ups. Waarom staat er op websites reclame en wat gebeurt er als je op die reclame klikt? Daarnaast wordt in dit hoofdstuk behandeld dat je niet zomaar op alles 'Ja' moet zeggen als iets gevraagd wordt.

Hoofdstuk 6 Digitaal pesten

Uit onderzoek blijkt dat er, net zoals op het schoolplein of bij de sportclub, ook wordt gepest via e-mail. In dit hoofdstuk leren je leerlingen wat het verschil is tussen pesten op het schoolplein en digitaal pesten. Ze leren hoe ze dit kunnen voorkomen en hoe ze ermee om kunnen gaan.

Hoofdstuk 7 Lang, langer, langst!

Rsi is een aandoening die niet alleen volwassenen kan treffen. Ook kinderen kunnen last krijgen van rsi. Dit kan door een verkeerde houding achter de pc, te lang/te vaak achter de pc of bijvoorbeeld te lang/te vaak achter de spelcomputer. In dit hoofdstuk leren kinderen hoe ze rsi kunnen voorkomen.

Hoofdstuk 8 Internet is cool

Wat mag wel en wat mag niet als het om internet gaat? En zijn er verschillen tussen

thuis en op school? Tijdens voorgaande lessen hebben de leerlingen veel geleerd over veilig omgaan met internet. Maar ook wat wel/niet mag op school of thuis. Als afsluiting gaan leerlingen zelf aan de slag met het maken van internetregels voor hun school en/of voor de thuissituatie.

Evaluatie

Alle kennis die de leerlingen de afgelopen lessen hebben opgedaan kan in een toets worden geëvalueerd.

3 Wat heb je nodig om de lessen te geven?

Iedere les zal gebruik worden gemaakt van een combinatie van verschillende soorten opdrachten. De lessen vinden niet constant achter de computer plaats. De reden hiervoor is dat niet alle scholen voldoende plaats en apparatuur hebben én omdat we het praten over dit thema (kinderen onderling en met jou als leerkracht) heel belangrijk vinden. Ook is het heel goed als leerlingen elkaar tips geven en met andere kinderen praten over problemen die ze bij het internetten tegenkomen.

3.1 Je (voor)kennis

Het lesmateriaal is zo geschreven dat je er zelf vast ook van leert. Veel leerkrachten hebben nu eenmaal niet de ervaring die kinderen hebben met internet. Hier voorziet deze handleiding in. Je vindt niet alleen de praktische informatie om de lessen goed te kunnen geven. Ook vind je aan het eind van iedere lesbeschrijving achtergrondinformatie over het onderwerp.

3.2 Leermiddelen

Per opdracht staan de leermiddelen genoemd die je nodig hebt. Dit varieert van pennen, papier, pc met internet tot zelfs aardappelzetmeel en jodium.

3.3 Lesaanpak

Om je een indruk te geven hoe je de lessen kunt inzetten en de opdrachten kunt uitvoeren, geven we een aantal voorbeelden.

Klassikaal

- Klassikaal de tekst van het lesboek doornemen en met de leerlingen bespreken.
- Via een beamer voorbeelden uit het lesboek laten zien.
- De opdrachten klassikaal voorbespreken en waar mogelijk de opdracht gezamenlijk uitvoeren.
- Na het maken van de opdrachten de antwoorden/oplossingen klassikaal bespreken. Dit kan eventueel met behulp van een beamer, waarmee je de online opdrachten bespreekt.

Individueel

- Leerlingen zelf de tekst laten doorlezen.
- Het onderwerp in de klas bespreken met de hele groep (klassikaal). Leerlingen de opdrachten individueel laten uitvoeren.
- Leerlingen de opdrachten als weektaak laten uitvoeren.
- Aan het eind van de week een moment vrijmaken om het behandelde onderwerp te bespreken met de klas (klassikaal).

3.4 De achtergrondinformatie

Op het einde van elk hoofdstuk vind je heel wat achtergrondinformatie. Het is niet de bedoeling dat je al die informatie beheerst, maar het is zeker aan te bevelen om die informatie voor elke les door te nemen. Soms wordt verwezen naar websites: wegens de constante actualisering van websites kan het mogelijk zijn dat occasioneel een bepaalde site niet meer beschikbaar is.

De achtergrondinfo wordt in kaders met een grijze achtergrond weergegeven.

3.5 Groepsgesprekken

Je zal merken dat er in de hoofdstukken wordt verwezen naar groepsgesprekken. Dit houdt in dat de leerlingen de kans krijgen met elkaar te praten over hun ervaringen op internet. Misschien dat het voor jou de eerste keer is dat in de klas een dergelijk gesprek over internet plaatsvindt? Een groepsgesprek over dit onderwerp waar kinderen veelal in thuis zijn loopt immers het beste als zij hun ervaringen kunnen vertellen aan een leerkracht die graag wil horen wat zij hebben meegemaakt en welke oplossingen ze hebben gevonden.

In de media wordt steeds vaker gesproken over een digitale kloof. Laat je echter geen digitale kloof aanpraten. Kinderen zijn inderdaad snel met de computer. Ze weten razendsnel te klikken en te msn-en. Maar als het gaat om omgaan met informatie of je gedragen op internet, zijn het de volwassenen die nog altijd een voorsprong hebben vanwege hun levenservaring. Internet is tenslotte een afspiegeling van de werkelijkheid. Ook op internet gelden omgangsregels en is het vanzelfsprekend dat je alert bent.

3.6 Opdrachten

De basisopdrachten

In het lesmateriaal zijn zowel online als offline opdrachten opgenomen. Offline wil zeggen dat daarbij geen computer nodig is.

Dit wordt in het lesboek aangegeven met de volgende symbolen:

- muis + pen voor online opdracht



- pen voor offline opdracht



Beschikt je school over een computerlokaal? Dan is dat natuurlijk een groot voordeel. Je kan de leerlingen tegelijkertijd de online opdrachten laten uitvoeren.

Beschik je over een aantal pc's per groep? Dan zal je de leerlingen moeten verdelen om de online opdrachten te kunnen maken. Dit kan op verschillende manieren. Het is in dat geval aan te bevelen om de opdrachten wel klassikaal door te nemen en te evalueren.

- Iedere leerling maakt de opdracht op een zelfgekozen moment in de week.
- Leerlingen worden opgedeeld in groepjes en maken per groepje de online opdrachten (hier geeft de leerkracht aan wie, wanneer een opdracht gaat maken).
- Leerlingen worden opgedeeld in groepjes. Eén groepje gaat de online opdracht maken, het andere groepje de offline opdracht. De groepjes rouleren.

Extra opdrachten

Het kan zijn dat je in je klas leerlingen heeft die snel door de opdrachten ‘heen’ zijn. Hiervoor zijn er aan het eind van een aantal hoofdstukken extra opdrachten. Je kan de opdrachten inzetten als extraatje, maar ook omdat je herhaling belangrijk vindt.

Opdrachten integreren in andere lessen – vakoverschrijdend werken

Er zijn diverse opdrachten die je kan integreren in andere lessen. Zo zijn er opdrachten waarbij de leerling een opstel moet schrijven, een rekensom maakt (waarbij je zelf wellicht nog meer voorbeelden kunt bedenken) en een chemieproef en splitpenpop moet maken. Door de opdrachten te integreren in andere lessen, kan je het onderwerp op diverse manieren laten terugkomen in de lesweek en ondertussen toch de reguliere lessen aanhouden.

Gemiddelde tijdsinvestering

Bij elk hoofdstuk wordt aangegeven wat ongeveer de gemiddelde tijdsinvestering voor het uitvoeren van de les en opdrachten is. Uit de praktijk blijkt dat de eerste twee hoofdstukken en het hoofdstuk over digitaal pesten meer aandacht vergen dan de andere hoofdstukken. Er wordt uitgegaan van een lesblok van 50 minuten.

3.6 De gebruikte websites

Wordt internet op school afgeschermd door middel van een inhoudsfilter? Dan is het belangrijk om voor aanvang van de lessen te controleren of alle websites, die worden genoemd in het lesmateriaal of die nodig zijn voor het maken van opdrachten, toegankelijk zijn.

Geen inhoudsfilter op school? Ook dan is het goed om zelf de opdrachten te maken, zodat je kan inschatten op welke websites de leerlingen terecht zullen komen.

Achteraan in deze handleiding vind je een lijst met interessante websites.

Achtergrondinformatie bij het inleidend hoofdstuk

Belgisch onderzoek

In België en Nederland zijn diverse onderzoeken gedaan en nog steeds gaande op het gebied van internet en kinderen/jongeren.

Wil je op de hoogte blijven van recente onderzoeken:

www.saferinternet.be → Pers

Hier lees je allerlei berichtgeving over internet en jongeren.

www.uvv.be/uvv5/pub/cinfo/jo/pdf/01.pdf

studie over internetgebruik bij jongeren.

www.insites.be/file.asp?filetype=doc/04/press_releases/20030424_NL_YOL.pdf

studie over internetgebruik bij jongeren.

Kinderen op internet

In 2002 maakte 41% van alle Belgische kinderen tussen de negen en elf jaar gebruik van internet (bron: Insites).

In Nederland maakte in 2005 maar liefst 75% van alle kinderen tussen 6 en 11 gebruik van het internet. In 2003 was dit nog maar 48%. (onderzoek: Sikkema 2005).

Dit geeft aan dat er een enorme groei is in het internetgebruik onder kinderen. Het percentage zal de komende jaren waarschijnlijk nog verder stijgen.

Dit zijn hun geliefde bezigheden zijn in volgorde:

1. MSN
2. Games
3. muziek downloaden
4. surfen
5. plaatjes zoeken
6. mailen

(bron: Kaboem!Media 2005. Onderzoek onder negen- tot vijftienjarigen)

Meer interessante onderzoeken:

Insites E-research & consulting, Youth online 5.0, 2007

www.hetjongerenonderzoek.nl van P. Sikkema (2005)

4 De lessen en opdrachten Niveau II

4.1 Hoofdstuk 1 Ik surf veilig

Doel:

- Leerlingen kunnen gericht de gewenste informatie zoeken op internet.
- Leerlingen kunnen analyseren of en wanneer de informatie betrouwbaar is.

Te behandelen onderwerpen:

- Wat zijn de favoriete websites van de leerlingen? Leuke dingen op internet.
- Minder leuke dingen op internet. Ervaringen uitwisselen.
- Hoe zoek je op internet?
- Vind je wat je zoekt op internet?

Gemiddelde tijdsinvestering: 1 lesuur

Opdracht 1

Titel: Zoek het antwoord op internet
Leermiddelen: pennen, pc met internetverbinding
Korte inhoud: De leerlingen gaan online op zoek naar het antwoord op de vraag 'Hoeveel mensen wonen er in België?' Het antwoord gaan ze zoeken via zoekmachines, startpagina's of andere portaalsites (vb. <http://www.aboutbelgium.net/>) of direct surfen naar voor de hand liggende websites.

Om zeker te weten of de gevonden informatie juist is, is het goed om minstens twee websites te vinden waar dezelfde informatie op staat. Dan kan er met enige zekerheid gesteld worden dat het antwoord juist is.

Natuurlijk zijn websites van betrouwbaar. Als je via Google zoekt, zal je vlug honderden sites vinden met informatie over het aantal inwoners. Websites van de overheid zijn dan natuurlijk betrouwbaarder dan eigen websites die gemaakt zijn door jongeren (homepages).

Bespreek met de leerlingen hoe ze het antwoord gevonden hebben, of ze op websites terecht kwamen die helemaal niets met het onderwerp te maken hadden, of ze websites met veel reclame zijn tegengekomen en waarom die reclame op de websites staat.

Laat de leerlingen ook inzien dat het jaartal van telling belangrijk is; zo krijg je immers ook verschillende getallen ...

- Zoeken via een zoekmachine, zoals
 - o Google (www.google.be) ,
 - o Zoek het eens op (users.skynet.be/zoekheteensop/)
 - o Kennisnet (www.kennisnet.nl).
 Tip: gebruik woorden ‘belgië’ en ‘inwoners’.
- Of via geavanceerd zoeken en de zin: ‘hoeveel inwoners heeft belgië?’
- Je kan ook zoeken via de encyclopedie Wikipedia (www.wikipedia.be)
- Zoeken via voor de hand liggende websites: www.belgie.be , www.statbel.fgov.be , ...

Antwoord: Antwoorden zijn te vinden op de volgende websites:
www.wikipedia.be
www.belgium.be
www.statbel.fgov.be (statistieken → bevolking).

2003	2004	2005	2006
10.355.844	10.396.421	10.445.852	10.511.382

Opdracht 2

Titel: Is alles waar?
 Leermiddelen: pennen, pc met internetverbinding
 Korte inhoud: Leerlingen krijgen vier foto’s van dieren te zien. Eén dier bestaat niet. Het dier is samengesteld uit twee andere dieren. De foto is dusdanig bewerkt dat het bijna niet te zien is dat het om twee foto’s gaat.

De leerlingen zullen minstens twee sites moeten zoeken waarop zij het antwoord op hun vraag kunnen vinden. Dan pas kun je met enige zekerheid zeggen dat het dier inderdaad bestaat of niet. Vervolgens kan je met de leerlingen bespreken hoe zij hebben gezocht, welke zoekwoorden zij hebben gebruikt en welke websites zijn gevonden en gebruikt.

Antwoord: *De geelkopraaf bestaat niet.*

Evaluatie

Wat hebben de leerlingen in deze les geleerd? Je kan met de leerlingen nogmaals bespreken waarover deze les ging.

Extra opdrachten

Titel: Verzin een vraag
Leermiddelen: pennen, pc met internetverbinding
Korte inhoud: Laat de kinderen een paar vragen opstellen, waarop zij een antwoord willen hebben. Of laat de kinderen elkaar een vraag stellen, die ze moeten opzoeken op internet. Je kan zelf richting geven aan het soort vragen dat gesteld wordt. Maak zoveel mogelijk gebruik van open vragen. Je kan ook zelf klassikaal een aantal vragen opstellen. Op deze manier bepaal je zelf op welke onderwerpen gezocht kan worden. Deze opdracht is een voorloper op de internetspeurtocht die aan het eind van de lessenreeks zal worden behandeld.

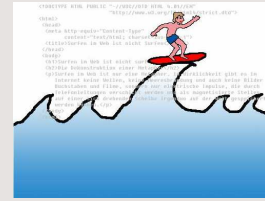
Titel: Internet is overal
Leermiddelen: pennen
Korte inhoud: Dagelijks worden we overal geconfronteerd met internet- adressen, op bijvoorbeeld televisie, in bladen, op de radio of op reclameborden en bussen. Welke internetadressen kunnen de leerlingen opsommen en waar hebben ze deze gehoord of gezien? Je kan dit als weekopdracht meegeven aan de kinderen. Laat de leerlingen ook tijdschriften meenemen en ga eens kijken hoeveel internetadressen daarin staan. Let er ook eens op hoeveel internetadressen je tegenkomt als je met de leerlingen op straat loopt, bijvoorbeeld naar de turnzaal, enz.

Achtergrondinformatie bij hoofdstuk 1

Surfen

Wat is surfen?

Surfen is volgens het internetwoordenboek 'het zwerven van de ene plek naar de andere op het World Wide Web'. Er is op internet genoeg te surfen. Kinderen gebruiken zoekmachines, startpagina's of gaan op de gok webadressen invullen.



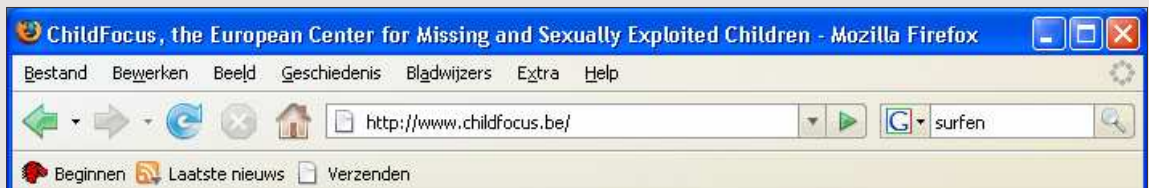
Zoekmachines zoals Google doen het werk om uit de vele websites die internet rijk is een keuze te maken en via startpagina's (portals of portalen) kan eenvoudig gezocht worden op onderwerp.

Goed zoeken is op zich al een kunst. Het heeft te maken met het bedenken van het juiste zoekwoord, om te vinden wat je zoekt. Dat geldt ook voor kinderen. Er zijn bijvoorbeeld lessen om zo efficiënt mogelijk te leren surfen en zoekmachines te gebruiken. Maar meestal is het toch vooral proberen om die websites te vinden die de informatie bieden die het kind zoekt.

Hoe gaat surfen in z'n werk?

Surfen kan als volgt gaan:

1. Het kind surft naar een **bepaalde website** door het adres van de site in te typen in de browser of bladerprogramma. Een browser is een programma waarmee websites op internet bekeken kunnen worden. Er zijn verschillende browsers, zoals Firefox, Opera, Netscape Navigator en Internet Explorer.



Kinderen weten dat er tussen de www en de .be of .com een bepaald woord moet staan. Dat is flink zoeken.

Bijvoorbeeld:

- Een kind is op zoek naar websites over olifanten en typt 'www.olifanten.be' in. Er verschijnt een site over o.a. inktpatronen. Hoe dit kan? Het komt vaak voor dat onder een domeinnaam een heel andere website schuil gaat dan verwacht. Bedrijven hebben deze domeinnamen geregistreerd, juist omdat het 'onschuldige' domeinnamen zijn waar veel mensen naar toe surfen. Uiteraard verwacht het bedrijf dat er verder gesurft wordt op deze website en links aangeklikt worden. Een andere mogelijkheid, 'www.olifant.be', geeft een site die nog niet is ingevuld
- Een ander voorbeeld is 'www.kat.be'. In elke klas is wel een leerling die een werkstuk over poezen wil maken en vervolgens op heel andere websites terecht komt, dan op websites over het huisdier ...

2. Het kind typt een zoekwoord in een **zoekmachine** in, om websites te vinden. Zoekmachine is de letterlijke vertaling van search engine. Bekende zoekmachines zijn Google (www.google.be), Yahoo (www.yahoo.nl), Advalvas

(www.advalvas.be) en Altavista (www.altavista.be).

In de zoekmachine wordt een zoekwoord ingetypt (in dit lesmateriaal wordt het woord 'zoekwoord' gebruikt, een andere term is 'trefwoord').

The screenshot shows a Google search interface. At the top left is the Google logo. To its right are navigation links: 'Het Internet', 'Afbeeldingen', 'Discussiegroepen', 'Nieuws', and 'meer >'. Below these is a search bar containing the word 'olifanten' and a 'Zoeken' button. To the right of the search bar are links for 'Geavanceerd zoeken' and 'Voorkeuren'. Below the search bar are radio buttons for 'het Internet' (selected), 'pagina's in het Nederlands', and 'pagina's uit België'. The search results are under the heading 'Het Internet' with 'Resultaten 1 - 10'. The first result is titled 'Olifanten' and has a snippet: 'Vlak voor 1980 waren er ongeveer 1,3 miljoen olifanten in Afrika. Daar is nu nog maar de helft van over. Stropers doden de dieren om het ivoor van de ...'. Below the snippet is a link: 'users.skynet.be/zoekheteensop/olifant.htm - 13k - In cache - Gelijkwaardige pagina's'. The second result is titled 'Welkom' and has a snippet: 'Tevens kun je hier veel informatie vinden over olifanten in het algemeen, vind je olifanten artikelen in de cadeaushop en kun je gratis mooie olifanten ...'. Below the snippet is a link: 'www.olifanten.org/ - 11k - In cache - Gelijkwaardige pagina's'.

The screenshot shows the Altavista search engine interface. At the top center is the Altavista logo. Below it are navigation tabs: 'Web' (selected), 'Afbeeldingen', 'MP3/audio', and 'Videobestanden'. Below the tabs is a search bar containing the word 'olifant' and a red 'ZOEKEN' button. To the right of the search bar are links for 'Geavanceerd zoeken' and 'Instellingen'. Below the search bar are radio buttons for 'ZOEKEN: Wereldwijd' and 'België' (selected). To the right of these are radio buttons for 'RESULTATEN IN: Alle talen' (selected) and 'Engels, Nederlands'. Below the search bar are links for 'Babel Fish Vertalen' and 'Meer >>'. At the bottom are links for 'Diensten voor Bedrijven', 'Een site aanmelden', 'Over AltaVista', 'Privacybeleid', and 'Help'. At the very bottom is the copyright notice '© 2007 Overture Services, Inc.' and a link for 'AltaVista in English'.

Alle websites waar het zoekwoord in voorkomt worden weergegeven. Hier kunnen ook ongewenste sites bij zijn, zoals pornosites.

3. Zoeken via een **startpagina**. Er zijn vele startpagina's (ook wel portals genoemd). Bijvoorbeeld www.startpagina.be, www.pagina.be, kids.startpagina.be en zo zijn er nog tal van portals.

Als voorbeeld gebruiken we www.pagina.be. Deze portal kent allerlei dochterpagina's. Op een dochterpagina staan websites met een bepaald thema. Bijvoorbeeld scholieren.be, sport.be. Op deze portals staan websites voor scholieren respectievelijk dierentuinen. Het zoeken via een startpagina kan een goede start zijn om websites over een bepaald thema te vinden.

The screenshot shows the website 'kids.startpagina.be'. At the top left is the logo for 'kids.startpagina.be' with the tagline 'de weg kwijt op het internet?'. Below the logo is a red 'aanverwante pagina's' button. To the right of this button are four columns of links: 'jeugd', 'peuter', 'kinderliedjes', 'kleurplaten', 'scouts'; 'diddl', 'kij', 'speelgoed', 'habbohotel', 'clown'; 'kinderfeest', 'harrypotter', 'neopets', 'plaatjes', 'metoyou'; and 'www.startpagina.be toevoegen aan favorieten', 'mijn.startpagina.be word moderator', 'moderator login'. Below these links is a search bar with a 'zoek' button. At the bottom are four yellow boxes: 'Kleurplaten' with links 'Kleurplaten.nl', 'Kleurplaten.org/', 'Diney.familiefun (EMC)'; 'Tv programma's' with links 'Winxclub.com', 'K3', 'Dinji.lanckoue'; 'Muziek' with links 'Clipjes', 'Songteksten.be', 'Radio.Bem.Bem'; and 'Sites voor kids' with links 'Turfjes', 'Speelzolder.com', 'Diet.Dicat.Schaap.schuit'.

4. Via andere websites. Vaak surfen kinderen van website naar website. Er staan links op een website en vervolgens klikken ze daarop om door te surfen. Kinderen zijn vaak niet op zoek naar bepaalde informatie, maar zijn meestal nieuwsgierig waar ze terechtkomen. Bijvoorbeeld een heel leuk spelletje.



Hoe werkt een zoekmachine?

Het woord dat gezocht wordt komt meestal op diverse pagina's voor. De zoekmachine geeft als resultaat die pagina's waar het woord op voorkomt. Omdat het om een woord gaat, wil het nog niet zeggen dat de gevonden webpagina's ook informatie bevatten die je zoekt. Het woord dat gezocht wordt komt op een pagina voor. De zoekmachine geeft als resultaat die ene pagina waar het woord op voor komt. Omdat het om een woord gaat, wil het nog niet zeggen dat de gevonden webpagina ook informatie bevat die je zoekt.

Zoeken met meerdere woorden heeft als voordeel dat al die woorden op één pagina moeten voorkomen. Wanneer de zoekwoorden 'olifant dierentuin' wordt opgegeven, dan moeten die twee woorden op één pagina voorkomen. De kans dat je dan op een webpagina van een dierentuin terechtkomt die over olifanten gaat is al een stuk groter geworden.

De zoekresultaten

worden op meerdere pagina's weergegeven. Hoe verder je gaat kijken, hoe minder de zoekresultaten met het onderwerp te maken hebben.

Een webpagina die het meeste aangeklikt wordt via een zoekmachine zal bovenaan de zoekresultaten verschijnen. Bedrijven kunnen ook adverteren, zodat hun webpagina altijd bovenaan in de zoekresultaten verschijnt.

Risico's

1. Kinderen zien ongewenste websites

Een kind kan geheel buiten zijn of haar 'schuld' om websites vinden die helemaal niet voor kinderen bedoeld zijn. Wie het zoekwoord 'poesjes' intypt in een zoekmachine, zal hoofdzakelijk websites vinden die niets met dit huisdier te maken hebben maar met seks. Al surfend kan een kind op websites komen die duidelijk niet voor kinderen zijn bedoeld. Ook kunnen kinderen bewust op ongewenste websites komen, omdat op internet nu eenmaal van alles staat en het gemakkelijk te vinden is. Niet alleen sekssites, maar ook discriminerende websites, websites met geweld e.d. In hoofdstuk 5 van het lesboek wordt hier uitgebreider op ingegaan.

2. Kinderen lezen via internet informatie die niet waar is

Niet alles wat is opgeschreven, is waar. Dat geldt voor papieren media zoals krant of tijdschrift, maar zeker ook voor internet. Er wordt heel wat gepubliceerd op internet. In feite kan iedereen die een eenvoudige website kan maken informatie op internet zetten. Anderen vinden en lezen die informatie. Het is belangrijk leerlingen te leren zichzelf de vraag te stellen: is het wel waar wat ik lees? Deze vraag wordt de kinderen aan de hand van opdrachten gesteld in de les over surfen.

Oplossingen

1. Kinderen zien ongewenste websites

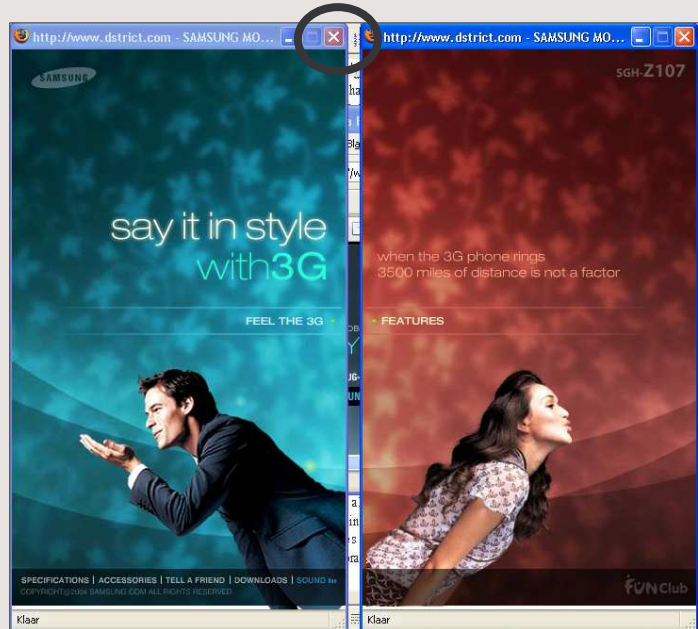
Dit kan op school gebeuren als je leerlingen aan het surfen zijn en het mogelijk is om naar diverse websites te zoeken. In deze situatie adviseren wij je om allereerst met de leerlingen afspraken te maken wat wel en wat niet tijdens de schooluren gedaan mag worden met internet. Voor de uitwerking van dit thema verwijzen we naar hoofdstuk 8 over internetgedragsregels. Het kan zijn dat je leerlingen, ondanks de afspraken, toch op een site komen met geweld, discriminatie of seks/porno/bloot. Ook tijdens de opdrachten in deze cursus. Praat er dan over met ze.

2. Kinderen lezen op websites informatie die niet waar is

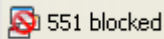
Het kan zijn dat je leerlingen opeens met (foutieve) informatie aankomen, waar je van denkt 'Hoe komen ze erbij?'. Het kan zijn dat ze (thuis of op school) zulke informatie hebben gevonden tijdens het surfen. Naast heel nuttige informatie staat er ook veel onzin op internet, maar dat onderscheid kunnen kinderen nog niet maken. Informatie die op internet te zien is moet (en kan) altijd gecontroleerd worden met informatie uit de bibliotheek en van de leerkracht. Juist het vergelijken van informatie is dé manier om erachter te komen of iets klopt of niet.

Pop-ups

Een pop-up is een advertentie die opeens op het scherm verschijnt als je een website bezoekt. Dit kan als je naar een website surft, of een website wilt wegklicken. Het is een manier om aandacht te vragen voor een product of dienst van bijvoorbeeld een sponsor van de site waarop je had geklikt. Andere pop-ups kunnen een onderdeel zijn van de website zelf, bijvoorbeeld om nieuwtjes onder de aandacht te brengen. Kinderen vinden de pop-ups meestal erg vervelend, want het hindert hen om snel door te surfen. Een pop-up kan vaak weg worden geklikt door, net als met een website, op het kruisje bovenaan te klikken. Maar dit lukt niet altijd. Sommige pop-ups (zoals de seksueel getinte advertenties) zijn zo hardnekkig dat de computer opnieuw moet worden gestart om de pop-ups kwijt te raken.



Oplossingen



Er zijn pop-up killers die je kan downloaden van internet en dan kan installeren op de pc. De meest bekende zijn de 'pop-up killers' in de werkbalk van bijvoorbeeld Google of MSN. Er zijn diverse browsers waar een pop-up killer is geïntegreerd in het programma. Dit zijn onder andere Firefox, Netscape en Opera. De ervaring leert dat kinderen graag willen vertellen over welke pop-ups ze zien en hoe vervelend ze dit vinden. Ga hierop in, laat hen vertellen. Er zijn namelijk ook pop-ups waarbij opeens betaald moet worden om een internetspel te kunnen spelen. Kinderen komen dan in de problemen, bijvoorbeeld omdat na een tijdje blijkt dat de telefoonrekening van de ouders erg hoog is. Let erop dat er voldoende ruimte is voor het verhaal van de kinderen en wellicht ook voor de oplossingen die ze zelf hebben bedacht.

Meer info op: <http://ludit.kuleuven.be/software/beveiliging/popup.html>

Vragen en antwoorden

Hoe open je een gesprek met leerlingen over (veilig) internetten?

Het is belangrijk dat je leerlingen de kans biedt hun verhalen te vertellen, zowel positief als negatief. Kinderen zijn vaak erg enthousiast over internet en dat willen we hen niet afnemen. Tegelijkertijd moet er ook plaats zijn om over slechte ervaringen en de oplossingen ervan te praten. Toon belangstelling voor wat de kinderen meemaken op internet en ze zullen je eerder om hulp vragen als er iets misgaat. Een opening kan bijvoorbeeld zijn: kunnen je leerlingen met elkaar een top 3 samenstellen van hun grootste irritaties op internet? Naar aanleiding van deze top 3 is er veel stof om door te praten. Maar ook de lessen op zich zijn vast voldoende om meer van je leerlingen te weten te komen en een gesprek hierover op gang te brengen.

Hoe zijn leerlingen te begeleiden als zij ongewild ongewenste sites bezoeken?

Leerlingen kunnen op sites terecht komen waar ze niet naar op zoek zijn. Het is belangrijk om hen te laten weten dat het terecht komen op zulke sites niet hun schuld hoeft te zijn: het kan iedereen gebeuren! Je leerlingen willen misschien graag uitleggen hoe het is gebeurd. Soms gaat dit lacherig. De achtergrond van de behoefte om het aan jou te laten zien, is dat zij er zeker van zijn dat zij niets fout hebben gedaan. Je kan met je klas de afspraak maken dat, als dit gebeurt, je op de hoogte wordt gesteld. Sommige leerlingen willen rustig doorsurfen, anderen hebben de behoefte over hun vervelende ervaring even na te praten.

Hoe zijn leerlingen te begeleiden als zij bewust ongewenste sites bezoeken?

Natuurlijk zijn leerlingen op ontdekkingstocht en ook bij jou in de klas zullen enkele kinderen juist op zoek gaan naar ongewenste sites. Dit is te vergelijken met de andere situaties die je als leerkracht al kent. Sommige leerlingen zullen de grenzen opzoeken. Je bent er als leerkracht verantwoordelijk voor dat jouw regels gelden. Ongewenste sites worden nu eenmaal niet opgezocht bij u in de klas. Het is aan jou of en zo ja welke consequenties je hieraan verbindt.

Hoe zijn ouders te begeleiden van wie de kinderen ongewenste sites op school hebben gezien?

Sommige leerkrachten hebben ouders op bezoek gekregen die bezorgd waren over het feit dat hun kind onder schooltijd op internet in aanraking is gekomen met ongewenste websites. Dit vergt geduld en uitleg. Natuurlijk is de school verantwoordelijk voor wat kinderen onder schooltijd doen, maar met internet ligt het net even iets anders. Je kan hen uitleggen welke internetregels er zijn en dat de school haar best doet om ook het internetten zo veilig mogelijk te laten verlopen.

Zijn ouders nog op een andere manier te betrekken bij dit thema?

Ja, je kan bijvoorbeeld een aparte ouderavond beleggen om samen met ouders te praten over internet op school en thuis. Ouders en leerkrachten kampen vaak met dezelfde problemen, omdat zij beiden op dit gebied veelal zijn ingehaald door hun leerlingen/kinderen. Misschien dat een ouder al mee helpt met de technische kant van internet. De medewerking van ouders kan erg meehelpen om een schoolbeleid op dit gebied vast te stellen. Er zijn verschillende organisaties die voorlichting aanbieden (zie eerder).

Tip: Wat weet jij van cyberveiligheid?

www.klasse.be/archief/index.php?op=archief&nr=9408

Hoofdstuk 2 Wat is e-mail?

Doel:

- Leerlingen zijn zich bewust van privacygevoelige informatie.
- Leerlingen kunnen omgaan met ongewenste e-mail.
- Leerlingen kunnen verklaren wat spam en 'doorstuur' e-mailtjes zijn.
- Leerlingen kunnen de kenmerken geven van een goed wachtwoord.

Te behandelen onderwerpen:

- Heb je een eigen e-mailadres? Aan wie geef je je e-mailadres?
- Ongewenste e-mail, van wie komt het en kun je het voorkomen? Vraag je ouders of je je e-mailadres mag doorgeven.
- Uitleg kraken.
- Hoe voorkom je het kraken van jouw account? Zorg voor goede wachtwoorden.
- Wat is een goed wachtwoord?
- Hoe onthoud je een goed wachtwoord?

Gemiddelde tijdsinvestering: 1 lesuur

Wat is ...

Account = een account bestaat uit een gebruikersnaam en een wachtwoord. Hiermee kan ingelogd worden bij een bepaalde dienst, bijvoorbeeld webmail, MSN, een spel of een profielwebsite.



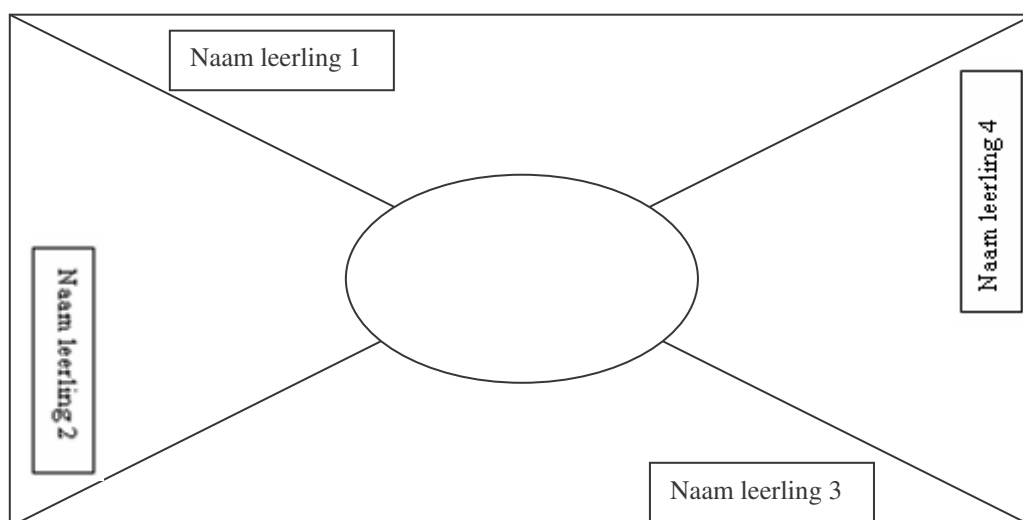
'Doorstuur' e-mailtjes = e-mail waarin gevraagd wordt het bericht naar zoveel mogelijk mensen door te sturen.

Evaluatie van de vorige les

Wat hebben we de vorige les gedaan en wat hebben we ervan geleerd?

Opdracht 3

- Titel: E-mailen
- Leermiddelen: pennen en groot vel papier
- Korte inhoud: Maak groepen van vier leerlingen. Iedere groep krijgt een vel papier waarop ze in het midden een rondje tekenen. De rest van het vel verdelen ze in vier vlakken. Laat de leerlingen zelf bedenken aan wie ze hun eigen e-mailadres zouden doorgeven. Ze schrijven dit elk in één vak op het papier. Laat de leerlingen overleggen wat ze hetzelfde hebben en wat niet. Laat ze in het rondje schrijven aan wie ze alle vier hun e-mailadres zouden doorgeven. Wanneer iedereen klaar is bespreek je met alle groepen aan wie je de e-mailadressen zou kunnen doorgeven.



Opdracht 4

- Titel: Gewone e-mail of niet?
- Leermiddelen: kleurpotloden, pc met internetverbinding.
- Korte inhoud: leuke e-mail of niet? Je legt aan de leerlingen uit dat ze leuke en minder leuke e-mail kunnen ontvangen. In het werkschrift staan e-mails van de 4 kinderen. De leerlingen kunnen met kleuren in het oefenboek aangeven wat ze vinden van de e-mails die de kinderen hebben gekregen. Na 10 minuten kan je met de leerlingen bespreken waarom ze een e-mail een bepaalde kleur hebben gegeven. Laat de leerlingen, die de begrippen nog niet beheersen, eerst de informatie op de websites overlopen, nl.

Spam: www.spamsquad.be

Hoax, virus: www.gva.be/dossiers/-c/computervirus/hoax.asp

- Antwoorden:
- Jonas: spam
- Laura: virus
- Muzaffer: gewone e-mail
- Tine: hoax

Opdracht 5

Titel:	Verzin een goed wachtwoord
Leermiddelen:	pennen
Korte inhoud:	<p>Je laat de leerlingen een wachtwoord verzinnen dat niet gemakkelijk te kraken is. Ze kunnen het wachtwoord ergens opschrijven, maar benadruk dat ze het niet moeten laten slingeren en leg nogmaals uit wat het belang is van een goed beveiligd wachtwoord. De leerlingen kunnen tot de volgende les proberen de wachtwoorden van de andere leerlingen te achterhalen. Je kan zelf ook meedoen met het verzinnen van een wachtwoord!</p> <p>In de periode tot de volgende les leren de leerlingen hoe ze hun wachtwoord geheim kunnen houden voor anderen. Je kan benadrukken dat het geven van wachtwoorden aan vriendinnen en vrienden niet aan te raden is. Ze hoeven maar even ruzie te hebben en de wachtwoorden worden misbruikt.</p> <p>In de volgende les bespreek je met de leerlingen of er wachtwoorden geraden zijn. Waarom sommige geraden zijn en andere niet. Hoe kun je wachtwoorden geheim houden?</p> <p>De spanning zit 'm in het feit dat de leerlingen iets moeten achterhalen, terwijl je weet dat de ander heel voorzichtig is!</p>

Extra opdrachten

Titel:	Wat is een goed wachtwoord?
Leermiddelen:	pennen
Korte inhoud:	<p>Om ervoor te zorgen dat een wachtwoord niet gekraakt (geraden of achterhaald) kan worden door een ander is het van belang een goed wachtwoord te verzinnen. Je legt aan de leerlingen uit wat het woord 'kraken' betekent. Vaak hebben je leerlingen deze ervaring zelf ook gehad; opnieuw raden we je aan om dit samen met de leerlingen te bespreken. Wiens wachtwoord is wel eens gekraakt? Hoe kwam dit? Wat hebben de kinderen hiertegen gedaan? Laat de leerlingen in het werkschrift schrijven waarom ze het gevonden wachtwoord goed of slecht vinden en wat ze anders zouden doen. Bespreek dit klassikaal.</p>

Antwoorden: *'TeiGertje' is een redelijk goed antwoord. De combinatie van hoofd- en kleine letters maakt het moeilijk te kraken. Gebruik liever niet een wachtwoord dat lijkt op de nickname die je gebruikt, en natuurlijk al helemaal niet jouw huisdier als wachtwoord (het blijkt dat kinderen vaak huisdieren gebruiken voor hun wachtwoorden!).*

Muzaffer1994 is een heel fout wachtwoord. Dat is namelijk zo te raden. Naam + geboortjaar.

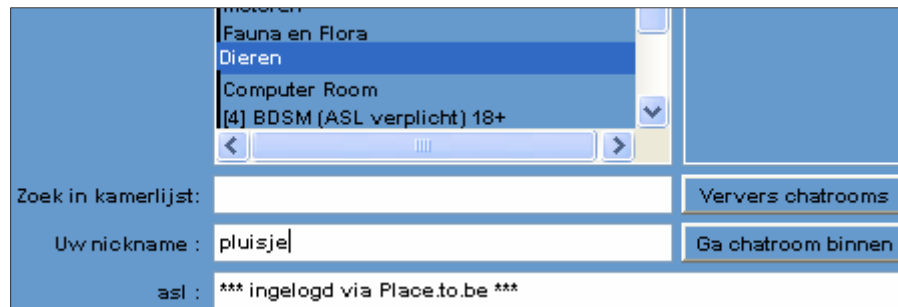
1-sanoj-2 is een goed wachtwoord. Combinatie van letters, cijfers en leestekens. De naam Jonas staat achterstevoren in het wachtwoord

MissLaura is geen goed wachtwoord. Ook al is er een combinatie

van hoofd- en kleine letters. Het is ook de bijnaam van Laura.
Kinderen kunnen dit dus prima weten!

Wat is ...

Nickname = de verzonden naam die het kind gebruikt als e-mailadres of als chatnaam. Nickname betekent 'bijnaam'. Vaak vinden kinderen het fantastisch om een nickname te bedenken.



The screenshot shows a chatroom interface with a list of chatrooms on the left and a search bar below it. The chatrooms listed are: 'Fauna en Flora', 'Dieren', 'Computer Room', and '[4] BDSM (ASL verplicht) 18+'. Below the list is a search bar with the text 'Zoek in kamerlijst:'. To the right of the search bar are two buttons: 'Ververs chatrooms' and 'Ga chatroom binnen'. Below the search bar is a field for 'Uw nickname:' with the text 'pluisje|'. At the bottom, there is a field for 'asl:' with the text '*** ingelogd via Place.to.be ***'.

Kraken = kinderen en andere internetgebruikers kunnen alleen met een gebruikersnaam en wachtwoord hun e-mail lezen of inloggen op MSN. Als iemand anders de accountgegevens kent of heeft geraden, noemen kinderen dit 'kraken'.

Titel: Wachtwoord

Leermiddelen: pc met internetverbinding

Korte inhoud: Tine is slordig met haar wachtwoord. De leerlingen proberen het wachtwoord van het karakter te kraken.
De leerlingen proberen achter het wachtwoord van Tine te komen. De nickname is in feite haar wachtwoord, maar dan op de juiste manier geschreven.
Je kan er een wedstrijd van maken ... Hoe sneller de leerlingen het antwoord van Tine hebben geraden, hoe 'slechter' Tine haar wachtwoord heeft verzonden! Ze moet dus op zoek naar een nieuw, ingewikkelder wachtwoord.
Laat leerlingen, die nog geen idee hebben hoe een goed wachtwoord wordt samengesteld, eerst deze website overlopen:

www.netonline.be/ict/detail.asp?id=343

Antwoord: *tijgertje*

Achtergrondinformatie bij hoofdstuk 2

E-mailen

Wat is e-mailen?

E-mailen is het versturen van een bericht met een e-mailprogramma via internet. Met een e-mailbericht kunnen bestanden worden meegestuurd, zowel tekst, beeld (stilstaand én bewegend) als geluid.

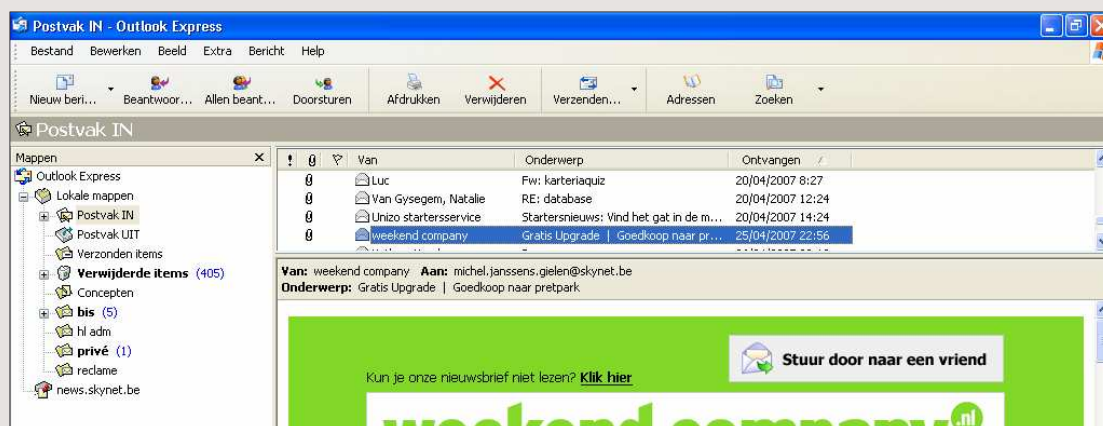
Kinderen verkiezen dan wel chatten boven mailen, maar als een ander kind (nog) niet op een chatbox zit, is een mailtje een goede manier om de ander iets te laten weten. Kinderen mailen ook met familie, bijvoorbeeld in het buitenland.

E-mailen kan met programma's zoals Thunderbird, Outlook Express, Eudora. E-mailen kan ook via webmail, zoals bijvoorbeeld Gmail, Hotmail of Yahoo. Je logt in op de website van de provider en je kan daar je mail lezen en berichten versturen. Voordeel is dat waar je op de wereld ook bent, je toegang hebt tot je webmail.

Hoe gaat e-mailen in zijn werk?

Via e-mail programma op pc:

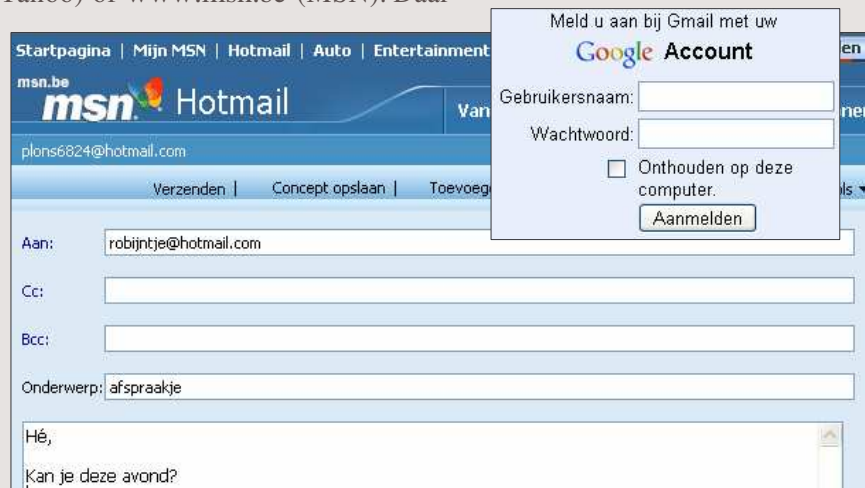
Kinderen gebruiken vaak het e-mailprogramma dat door de ouders wordt gebruikt. Het komt vaak voor dat gezinsleden hun eigen e-mailadres hebben. Het kan zijn dat de e-mail voor alle adressen in één programma binnenkomt, maar het kan ook zijn dat er verschillende gebruikers aangemaakt zijn, waardoor de gezinsleden niet elkaars e-mail kunnen lezen.



Via webmail online:

Bij de tweede mogelijkheid surft een kind naar de website van zijn of haar provider, bijvoorbeeld www.gmail.com (Gmail) www.hotmail.com (Hotmail), www.yahoo.com (Yahoo) of www.msn.be (MSN). Daar

typt het de inlognaam en het wachtwoord in, om vervolgens de post te lezen en te beantwoorden. Anderen die niet over deze gegevens beschikken kunnen de e-mail niet lezen.



E-mailen op school

Er zijn leerlingen die vanuit school een e-mailadres hebben gekregen. Bedoeling is vaak om het te gebruiken voor schoolzaken. Ze zijn vaak gebaseerd op webmail.

Risico's

Een kind krijgt ongewenste e-mail

Een kind kan een e-mailtje ontvangen waar het helemaal niet op zit te wachten. Dat kunnen bijvoorbeeld reclameboodschappen zijn. Hiervoor is het niet altijd nodig dat de ander het e-mailadres van het kind in bezit heeft. Er zijn bedrijven die allerlei trucs uithalen om mensen te bereiken. Men spreekt in dit geval ook van 'spam'.



Cross J.Rita

[SPAM] In the spring, the sun rises earlier each day.

wo 2-5-2007 16:38

21 kB

2 Een kind krijgt pestmailtjes

Het pesten is van de speelplaats uitgebreid naar de virtuele wereld, waar ook kinderen elkaar ontmoeten. Je moet je voorstellen, dat een pestmailtje scheldwoorden bevat die speciaal gericht zijn tegen het betreffende kind. Het kind leest de nare e-mail in een voor hem of haar veilige omgeving, wat nog kwetsbaarder maakt. Zulke e-mailtjes zijn soms anoniem verzonden. Een weerwoord is niet mogelijk. Pestmailtjes zijn heel naar voor een kind en een kind kan zich daardoor erg kwetsbaar voelen. In hoofdstuk 6 gaan we dieper in op dit thema.

3 Doorstuurmailtjes en nepberichten.

De meeste kinderen zullen ze wel kennen. De doorstuurmailtjes (ofwel kettingsbrieven) per e-mail. Soms worden kinderen én volwassenen bedolven onder deze berichten. De berichten zien eruit zoals we ze misschien zelf nog kennen uit onze eigen jeugd. Er wordt gesteld dat het bericht naar een minimaal aantal personen doorgestuurd moet worden, want anders... kan er van alles gebeuren of heb je geen geluk in je leven.

Daarnaast zijn er de nepberichten, waarin vaak zielige verhalen worden verteld, met daarbij de vraag om het bericht aan zoveel mogelijk mensen door te sturen. Het doorsturen van al die e-mails is nog niet zo'n ramp, maar het feit dat boven de berichten waslijsten met e-mailadressen ontstaan wel. Deze adressen kunnen door iedereen gebruikt worden. Komt een dergelijke mail met een waslijst aan e-mailadressen bij een spammer (bedrijf of particulier die ongevraagd reclame-mail verstuurt) terecht, dan zullen ze je dankbaar zijn.

Van: Jef Essers **Aan:** albert ruiters; andre vandezavel; Annie Van Lier; rene essers; rudi lenaerts; erwin dewelf; Ivan Wolters; Ivon Roefflaer; Inf...
Onderwerp: Doorst.: FW: Doorst.: FW: terugsturen als jij het ook meent !!!!!



Daarnaast kan het voorkomen dat dergelijke berichten op een pc blijven staan die besmet is met een virus. Het virus kan zichzelf verspreiden via alle e-mailadressen in het bericht.

Oplossingen

Privacy?

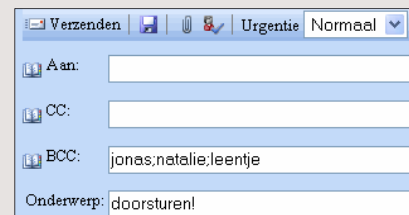
Het aspect veiligheid is vaak een argument om het gebruik van e-mail te beperken. Het communicatiemiddel van virussen aantrekken en de veiligheid van het schoolnetwerk in gevaar brengen. E-mail kan leerlingen ook blootstellen aan reclame. De school kan dergelijke risico's echter vermijden met een doordachte instelling van de e-mail.

De leraar kan er ook voor zorgen dat alle e-mail die verstuurd of ontvangen wordt via hem of haar passeert. Zo'n aanpak is een aanrader voor de eerste graad van het secundair onderwijs, die erop moeten toezien dat de kinderen niet in contact komen met ongewenste e-mails. Jongeren in het secundair daarentegen, zouden het beschouwen als een inbreuk op hun privacy als de leraar hun e-mails leest. Tenzij op voorhand duidelijk is dat er op de computers van de school geen persoonlijke e-mail wordt verstuurd. Zo'n afspraak is makkelijk te realiseren door een klassikaal e-mailadres te gebruiken.

Spam

Iedereen met een e-mailadres krijgt (wel eens) e-mail van mensen die hij of zij helemaal niet kent. Daar zit nogal wat ongewenste e-mail bij, bijvoorbeeld reclame. De oorzaak kan enerzijds zijn dat de persoon in kwestie wat al te gemakkelijk om is gegaan met het eigen e-mailadres (door het bijvoorbeeld achter te laten op een website). Maar dit hoeft beslist niet altijd op te gaan. Bedrijven combineren namelijk allerlei gegevens om reclame te kunnen versturen. Er is wel een aantal tips om zoveel mogelijk te voorkomen dat het eigen e-mailadres gemakkelijk te bereiken is.

- Verzin een gebruikersnaam (de naam die voor @ komt te staan). Het is belangrijk dat e-mailadressen (zeker van kinderen) niet traceerbaar zijn. De echte voor- en achternaam is dus niet raadzaam! Laat kinderen liever een naam verzinnen. Elke kind heeft wel een aparte 'nickname' (bijnaam). Het is nog spannender ook om met die bijnaam te mailen!
- Dit geldt ook voor e-mailadressen vanuit school. Als school moet je er ook voor zorgen dat de leerlingen niet zomaar door anderen te traceren zijn. Het aanleren van privacy geldt ook voor het maken van e-mailadressen op school. Dus niet: jan.jansen@bernardusschool.be maar bijvoorbeeld wel: groep8_115@bernardusschool.nl. Dan nog is de leerling te traceren. Via een zoekmachine is het vrij eenvoudig te achterhalen waar de school zich bevindt en niet veel later waar het kind woont. Tenslotte wonen kinderen nooit erg ver van hun school vandaan.
- Wees voorzichtig en zuinig met het achterlaten van het e-mailadres op internet. Het is raadzaam voor kinderen om dit op voorhand altijd te overleggen met hun ouders of leerkracht. Beter nog is het om een tweede e-mailadres aan te maken dat alleen gebruikt wordt om op internet door te geven. Ontvangt het kind te veel spam op dit adres, dan kan het een ander account aanmaken en het vorige account verwijderen.
- Als er toch reclamemail wordt gestuurd, beantwoord deze nooit: dit is voor de bedrijven vaak een manier om erachter te komen of de reclame inderdaad is aangekomen! Hierna wordt er nog veel meer e-mail gestuurd.
- Stuur geen nepberichten of doorstuurmailtjes door. Ze zijn echt onzin. Wil je het toch doorsturen, let er dan op dat je alle e-mailadressen achter 'BCC' invult en niet allemaal achter 'Aan'.



The image shows a screenshot of an email composition window. At the top, there is a 'Verzenden' button and a dropdown menu for 'Urgentie' set to 'Normaal'. Below this are fields for 'Aan:', 'CC:', and 'BCC:'. The 'BCC:' field is filled with the text 'jonas,natalie,leentje'. The 'Onderwerp:' field is filled with 'doorsturen!'.

Wat kan ertegen gedaan worden?

Kinderen behoren allereerst te weten dat ze niet pertinent 'schuld' hebben als ze ongewenste e-mail ontvangen. Er kan heel wat anders aan de hand zijn, bijvoorbeeld een situatie die we hierboven hebben besproken.

In geval van pesten: Bewaar de e-mail!

Het is raadzaam kinderen te vertellen om eventueel de vervelende e-mails te bewaren. Als ze hulp of steun zoeken bij opvoeders is het belangrijk dat de opvoeders het bericht kunnen nalezen. Bovendien, als het helemaal uit de hand loopt, en er moet aangifte gedaan worden bij de politie, wordt het bestand opgevraagd.

Er zijn technische tips om ongewenste mail te voorkomen:

Blokkeren van ongewenste e-mail

De kinderen leren in de les over e-mailen hoe zij kunnen blokkeren. Het is raadzaam om aan kinderen te leren dat zij altijd een e-mailadres moeten gebruiken waarmee geblokkeerd kan worden. Er zijn veel e-mailprogramma's en webmailvarianten, dus ook vele manieren om te kunnen blokkeren. Gelukkig staan de mogelijkheden om dit te doen vaak goed aangegeven in het menu. E-mailt het kind met hotmail (wat heel veel kinderen doen)? Kijk in 'Postvak In' en klik op 'Ongewenst'.

Op de website www.microsoft.com/belux/nl/athome/security/default.msp vind je videofragmenten en allerlei nuttige informatie om dit thema te stofferen.



Vragen en antwoorden

Wat is webmail?

Webmail is de manier om e-mail te lezen en te versturen via een website. Bijvoorbeeld: het Gmail-adres wordt bekeken via www.gmail.com, een Yahoo-adres wordt gelezen via www.yahoo.com en Hotmail via www.hotmail.com.

Is webmail veiliger dan een mailprogramma?

Zo simpel ligt het niet. Het is belangrijk dat een kind zijn of haar privé-gegevens beschermt en e-mailt met een verzonden naam; of dit nu via een webmailadres is of via een e-mailprogramma op de pc. We adviseren altijd een e-mailprogramma of webmail te gebruiken waarin geblokkeerd kan worden. Op die manier kan het kind namelijk vervelende e-mail van een bepaalde afzender blokkeren.

Is blokkeren de ultieme oplossing?

Nee. Feit is dat pesten helaas een veelvoorkomend verschijnsel is. Pesten via internet dus ook. Blokkeren van een pestende mailer helpt, omdat het kind de nare e-mails niet meer hoeft te ontvangen. (Tenzij de pester gewoon via een ander e-mailadres doorgaat met pesten.) Het helpt een beetje, maar het gevoel gepest te worden blijft: er zijn namelijk weinig kinderen die alleen maar via internet gepest worden. De combinatie met het andere pesten (op sportclub of speelplaats) blijft.

Uit recent onderzoek (UIA 2006) blijkt dat in Vlaamse scholen gemiddeld één kind op de vijf wordt gepest. Het gaat om bijna 1 op de 4 (23%) van alle leerlingen uit het lager onderwijs en 1 op de 7 (15%) van alle leerlingen uit het secundair onderwijs. In het totaal 155.000 kinderen. Pesten komt het vaakst voor bij kinderen tussen 10 en 14 jaar. Ten minste 1 kind op de 20 krijgt wekelijks tot zelfs dagelijks met pesterijen af te rekenen. Het aantal pestkoppen ligt ook behoorlijk hoog. 15.9 % van de kinderen in het basisonderwijs en 12.3% van de jongeren in het secundair onderwijs pest andere leerlingen. Gemiddeld telt daarmee elke Vlaamse klas een leerling die pest en een leerling die gepest wordt. Cijfers wijzen uit dat jongens meer pesten dan meisjes. Jongens doen dat veeleer op een directe manier: uitschelden, pijn doen, eigendommen van leerlingen beschadigen ... Meisjes pesten minder vaak en geven de voorkeur aan indirecte pesterijen, zonder dat het tot een zichtbaar treffen komt: roddelen, uitsluiten, leugens rondstrooien, venijnige opmerkingen maken. Daarom treffen we bij het cyberpesten relatief gezien meer meisjes aan. De pesterijen vinden in iets meer dan de helft van de gevallen plaats in de eigen klasgroep, vooral op ogenblikken dat de groep min of meer ontsnapt aan het toezicht van volwassenen, bijvoorbeeld tijdens het speelkwartier en de middagpauze. (Bron: www.cyberpesten.be)

Wie kan de afzender opsporen?

De pester zal in de meeste gevallen iemand uit de directe omgeving zijn. Vaak is het een klasgenoot, iemand uit de wijk, iemand van de sportclub. Samen met het kind kan je naar de inhoud van de e-mail kijken en naar het e-mailadres waarmee het verstuurd is. Het kan zomaar zijn dat je al in de gaten hebt wie de pester is.

Een groepsgesprek in de klas kan helpen om het pesten te stoppen. Praten over deze gemene vorm van pesten en het bespreekbaar maken dat de pester te traceren is kan er toe leiden dat de pester ophoudt of zelfs toegeeft te pesten.

In ernstige gevallen van stelselmatig pesten kan aangifte gedaan worden. Indien niet bekend is wie de e-mails verstuurt, kan de politie via providers achter de identiteit van de pester komen. Deze gegevens mag een provider echter alleen geven nadat er aangifte is gedaan en justitie er om vraagt. Het is goed om te weten dat de politie de originele e-mails moet hebben. In de e-mails zit namelijk code verborgen (niet direct zichtbaar) waarmee de verzender getraceerd kan worden.

Wat is de Robinson-lijst?

Iedereen heeft in principe het recht om reclame via e-mail te weigeren. Totnogtoe bestonden er geen procedures om je te verzetten tegen reclameboodschappen die je via e-mail ontvangt. Het Belgisch Direct Marketingverbod (BDMV) werkt nu echter aan een lijst waarop iedereen kan intekenen die reclame via e-mail of sms beu is. Het initiatief is een uitbreiding van de zogenaamde Robinsonlijst tegen ongewenste telefoon- en postreclame. Je kan het vergelijken met de “geen ongeadresseerd reclamedrukwerk”-sticker op je voordeur.

Je kan op het internet je adres toevoegen aan de Robinson e-mail dienst.

Tachtig procent van de direct marketingbedrijven zou zich aan de deontologische code houden.

Meer info op www.robinsonlist.be

Hoofdstuk 3 Wie ben jij op internet?

Doel:

- Leerlingen kunnen omschrijven wat privé-gegevens zijn.
- Leerlingen zijn zich ervan bewust hoe om te gaan met het verstrekken van privé-gegevens op internet.
- Leerlingen zijn zich bewust dat personen zich anders kunnen voordoen dan ze zijn op internet.
- Leerlingen zijn zich bewust dat ze geen privé-gegevens doorgeven via chatboxen.
- Leerlingen zijn zich bewust dat niet alles wat online staat op waarheid berust.
- Leerlingen zijn zich bewust dat ze veilig kunnen chatten m.b.v. hun eID.

Te behandelen onderwerpen:

- Definities privé-gegevens vaststellen.
- Aan wie geef je wel/geen privé-gegevens door? Waarom geef je wel/geen privé-gegevens?
- Wat geef je door via een chatbox?
- Is alles wat op internet staat ook waar?
- Wat is de eID (elektronische identiteitskaart)?

Gemiddelde tijdsinvestering: 1 lesuur

Evaluatie van de vorige les

Wat hebben we de vorige les gedaan en wat hebben we ervan geleerd?

Opdracht 6

Titel: Privé-gegevens

Leermiddelen: kleurpotloden

Korte inhoud: Bespreek met de leerlingen wat privé-gegevens zijn.

- Waarom moet je voorzichtig zijn met de bekendmaking van privé-gegevens?
- Wat kunnen de gevolgen zijn wanneer je privé-gegevens op internet vermeldt?
- Welke gegevens zet je wel en welke kun je beter niet op internet zetten en waarom is dat?

Op het werkblad zijn privé-gegevens in tekstwolken door elkaar vermeld die de leerlingen kunnen inkleuren. Daarmee geven ze aan welke gegevens ze wel en niet zouden doorgeven aan iemand op internet. Bespreek daarna waarom ze tot die keuze zijn gekomen.

Rood = *niet doorgeven op internet*

Oranje = *ik weet het niet zeker*

Groen = *wel doorgeven op internet*

Opdracht 7

Titel:	Nickname
Leermiddelen:	pennen en pc met internetverbinding
Korte inhoud:	<p>In het werkschrift staat een lijst met nicknames. De leerling bekijkt de nicknames en bedenkt welke nicknames volgens hem/haar geschikt of ongeschikt zijn.</p> <p>Een nickname kan veel zeggen over de gebruiker achter de naam. Maar een nickname kan ook een heel verkeerde indruk geven van deze persoon. Bijvoorbeeld: 'sandra18' wekt direct de indruk dat je een meisje bent van 18 jaar oud. Zo kan de nickname 'sexygirl' de indruk wekken dat je te maken hebt met een meisje dat zich graag laat zien Waarom geven nicknames soms een verkeerde indruk en wat zijn goede nicknames?</p> <p>Een goede nickname is een nickname waarin:</p> <ul style="list-style-type: none">- geen voor- en achternaam is gebruikt- geen voornaam en geboortjaar of leeftijd zijn gebruikt- geen woorden staan die een 'verkeerde' indruk kunnen- maken, zoals sexy namen als 'stoeipoes', 'grotejan' e.d. (vooral kinderen die de puberteit ingaan, willen zich graag met dit soort namen profileren op internet).

Antwoorden: Goede nicknames zijn:

Horselover

DragonAX

Whizzy

amigo

digi

Goudvisje

ikke

skater

Just_me

Opdracht 8

Titel:	Wie ben ik?
Leermiddelen:	pennen
Korte inhoud:	<p>Rollenspel. Drie leerlingen krijgen van jou de opdracht om zich voor te doen als iemand anders. Van te voren heeft de leerling opgeschreven wie hij/zij is. Ze spelen bijvoorbeeld een ander kind uit de klas of een bekende Vlaming. De andere leerlingen in de klas moeten erachter komen wie ze zijn. Dit kan alleen door goede vragen te stellen. De 'onbekende' moet natuurlijk zo weinig mogelijk loslaten, maar alle vragen moeten wel beantwoord worden. Kinderen leren dat als zij eerlijk antwoord geven op de vragen, achterhaald kan worden wie ze zijn, waar ze wonen etc. Je kan dit spel vergelijken met het bekende televisieprogramma 'Wie ben ik' dat jarenlang op de televisie is geweest.</p>

Extra opdrachten

Titel: Nog meer nicknames
Leermiddelen: Bord, pennen en papier
Korte inhoud: De leerlingen schrijven op een papiertje hun naam en een nickname die ze zelf kiezen. De leerkracht heeft de bedoeling niet op voorhand aan de leerlingen verteld. De leerlingen mogen hun nickname niet aan de andere leerlingen tonen of zeggen. Dan schrijft de leerkracht in willekeurige volgorde de nicknames op bord. Tenslotte overloopt de leerkracht de nicknames op bord één voor één; telkens laat de leerkracht de klas raden naar de leerling die achter de nickname zit. Bedoeling is de leerlingen te laten inzien dat sommige zich heel bloot geven op het internet, terwijl anderen zich dan weer heel anders voordoen.

Titel: Cammen
Leermiddelen: pc met internetverbinding
Korte inhoud: Er wordt in deze opdracht ingegaan op het gebruik van een webcam. Tine wordt op een chatbox gevraagd om iemand toe te voegen aan haar MSN en de webcam aan te zetten. De leerlingen kunnen hun keuze maken wat Tine zou moeten doen.

Titel: eID kwis
Leermiddelen: pennen, pc met internetverbinding
Korte inhoud: Bespreek nogmaals het begrip eID; leg heerbij de nadruk op de mogelijkheid om veilig te chatten. Alle leerlingen van 12 tot 15 jaar hebben deze mogelijkheid. De leerlingen maken groepjes van twee tot vier leerlingen. Vervolgens mogen ze de vragen uit het oefenboek om ter snelst oplossen. Het groepje dat als eerste alle vragen juist heeft opgelost, is gewonnen. De leerkracht kijkt de oplossingen na; als er één of meer fouten zijn, moeten ze verder werken. De leerkracht kan ervoor kiezen om niet te zeggen welke vraag fout is beantwoord. Dit maakt het natuurlijk moeilijker. De leerlingen kunnen eventueel aan de computer het antwoord opzoeken. Ze kunnen daarbij een beroep doen op de websites:

- <http://eid.belgium.be/nl/navigation/documents/42993.html>
- www.eidsite.be/node/32
- www.saferchat.be

Antwoorden: 1: b / 2: a / 3 : b / 4 : a / 5 : a

Achtergrondinformatie bij hoofdstuk 3

Privé-gegevens en chatten

Chatten

Chatten betekent kletsen op internet. Chatten kan worden beschouwd als een nieuwe, moderne manier van communicatie.

Kinderen maken met elkaar contact via een chatbox, MSN, enz. MSN is de favoriete bezigheid van kinderen op internet. Ze onderhouden er hun sociale contacten.

Kinderen experimenteren regelmatig door onbekenden toe te laten op hun MSN. Hoe ouder de kinderen worden, hoe meer ze geleerd hebben dat vooral contacten met bekenden leuk zijn.

Voorbeelden van chatboxen:

www.msn.be, www.place.to.be,
www.saferchat.be,
www.jongerenplaneet.be,



Onschuldig?

De beste manier om op het internet mensen te ontmoeten is via een informele babbel in een chatruimte. Occasioneel leiden chatsessies ook tot reële ontmoetingen en nieuwe relaties. Er zijn op het internet ook speciale daterooms of chatruimtes die bedoeld zijn voor amoureuze doeleinden. Ook scholieren flirten behoorlijk wat af op het internet, al dan niet via een dateroom. Het virtuele geflirt in de chatruimte is op zich een stuk onschuldiger dan wat zich aan de schoolpoort afspeelt. Aan chatrooms is echter ook een risico verbonden. Pedofielen die actief zijn op het internet begeben zich vaak naar chatruimtes die voor jongeren bestemd zijn. Ze spreken er de aanwezige kinderen aan, doen zich voor als een aardig leeftijdsgenootje en bouwen langzaam een vertrouwensrelatie op. Eenmaal het slachtoffer voldoende vertrouwen heeft, is het voor de pedofiel niet moeilijk om kinderen te bewegen tot een echte afspraak.

Wat zeg je best niet?

Het is voor kinderen moeilijk om zelf te bedenken wat privé is en wat niet. Ga zelf maar na: kinderen hebben immers weinig privacy. Ze wonen bij hun ouders, op het adres en in het huis van hun ouders, met het vaste telefoonnummer van hun ouders.

Meestal vinden kinderen dat wat 'met hun ouders te maken heeft' wel privé was. Dat betekent dat deze kinderen niet het vaste telefoonnummer tijdens een chat gaven, maar hun eigen GSM-nummer wel. Ofwel: het is belangrijk om je leerlingen te leren wat privacy is. Dat kan alleen als zij doorkrijgen hoe kwetsbaar ze op internet kunnen zijn.

In het lesmateriaal zien de leerlingen hoe de 4 kinderen van de cursus voorzichtig omspringen met hun gegevens en welke onverwachte gevolgen dit kan hebben. Op internet kan iedereen zich immers anders voordoen. Dat maakt het voor kinderen moeilijk om niet naïef en goedgegelovig te zijn en de ander (ook al ziet hij/zij de ander niet) niet zomaar op zijn woord te geloven. We draaien het om: laten we de kinderen leren zich te beschermen op internet, bijvoorbeeld tijdens een chat, door zich anoniem te gedragen.

Jongeren chatten anderhalf uur per dag en vooral over seks



Hoe kunnen privé-gegevens in een chat worden weggegeven?

Kinderen moeten voor ze kunnen chatten enkele gegevens intypen. Hun naam, soms hun leeftijd, e.d. Gelukkig hebben de meeste kinderen wel door dat dit niet hun echte naam moet zijn, maar een verzonnen naam: een zogenaamde nickname.

Uw nickname :	<input type="text" value="whizzy"/>	<input type="button" value="Ga chatroom binnen"/>
asl :	*** ingelogd via Place.to.be ***	

Tijdens het chatten kunnen de kinderen een leuke persoon tegenkomen die ze graag willen leren kennen. Dan wordt het voor een kind moeilijk om zich in te houden en niets over zichzelf te vertellen. Zo kan er gevraagd worden om de ander toe te voegen aan hun MSN, een foto van henzelf te sturen of de webcam te gebruiken.

Een metafoor die je kan gebruiken is bijvoorbeeld de krant. Zou je een bepaalde foto van jezelf op de voorpagina van de krant zetten? Nee? Dan kun je het beter ook niet op internet doen. Tenslotte kunnen op internet nog veel meer mensen meekijken.

Hetzelfde geldt voor het doorgeven van privé-gegevens aan een vreemde op straat. Zou je die vreemde vertellen waar je woont, je telefoonnummer en je foto meegeven? Nee? Waarom zou je het dan wel doen op internet?

Risico's

Kinderen geven ongemerkt privacygevoelige informatie weg. Dit kunnen e-mailadressen zijn en telefoonnummers, maar ook huisadres of foto's van zichzelf.

De risico's zijn bijvoorbeeld:

- Een kind krijgt onverwachte e-mail, sms-jes, of telefoontjes. Let wel: dit hoeft niet pertinent ongewenst te zijn! Een kind kan namelijk vinden dat het met een leuke persoon aan de praat is geraakt tijdens het chatten.
- Een kind krijgt allemaal spam. De oorzaak is wellicht dat het kind zijn/haar e-mailadres heeft achtergelaten. Commerciële websites zijn heel handig in het 'aftroggelen' van gegevens, en kinderen willen die vaak geven in ruil voor een in het vooruitzicht gesteld cadeautje.
- Een kind heeft foto's doorgestuurd en ziet dat een foto misbruikt is voor andere doeleinden. Bijvoorbeeld doordat het op een profielwebsite is gezet of bewerkt en doorgemailed naar anderen.
- De webcamsessie is door de ander opgenomen en wordt in een later stadium gebruikt als chantagemiddel om iets voor elkaar te krijgen bij het kind.
- Een kind krijgt bezoek thuis. Dat is schrikken, want een kind rekent er misschien niet op dat het weggeven van zijn/haar huisadres tot gevolg kan hebben dat er ook daadwerkelijk aan de deurbel gebeld kan worden. Toch gebeurt dit.

Kan dit worden voorkomen?

Zoals gezegd: kinderen moeten leren wanneer het onverstandig is om privé-gegevens op internet achter te laten of door te geven. Een uitspraak van een kind willen we je niet onthouden:

“Privé is alles wat van mij is en waar een ander niets mee te maken heeft”

Met deze uitspraak in de hand kan je al een hele discussie met kinderen krijgen. Want wat is 'van mij', of waar heeft 'een ander niets mee te maken'? Dat ligt voor kinderen anders dan voor volwassenen, want zij leven immers in een heel andere wereld. De kern van het probleem is dat kinderen niet in de gaten (kunnen) hebben hoe zij te traceren zijn. Daarom doen we dit tijdens de lessen voor. Het is aan te raden om zelf te zien hoe gemakkelijk je aan persoonsgegevens kunt komen via internet.

Oplossingen

Hoe kunnen kinderen in hun privacy beschermd worden? Dat is de hamvraag! Ze moeten leren hoe ze dit moeten aanpakken. Net zoals ze zich leren bewegen in het verkeer, waar ze zich aan bepaalde regels moeten houden.

Hoe?

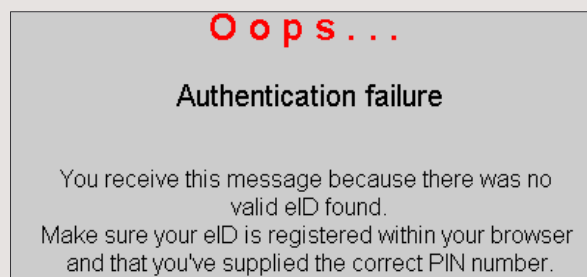
- Door niet zomaar privé-gegevens zoals: echte naam (voor- en achternaam), adres, telefoonnummers, foto's weg te geven.
- Door geen gegevens door te geven waarmee ze te traceren zijn. Bijvoorbeeld schoolnaam, sportclub (en tijden dat ze daar sporten bijvoorbeeld), namen van broers/zussen/vader/moeder e.d.
- Door een tweede e-mailadres aan te maken, dat doorgegeven kan worden op commerciële websites. Bijvoorbeeld om aan een wedstrijd te kunnen meedoen. Ontvangt het kind te veel spam op dat adres, dan kan het adres verwijderd worden en een nieuw adres aangemaakt worden.
- Door geen onbekenden toe te laten op MSN. Of, als ze dat wel graag willen, een tweede account aan te maken, zodat ze daar onbekenden aan kunnen toevoegen.
- Door de webcam niet te gebruiken bij een onbekende. Je weet niet wat de ander doet met de beelden of wat de ander precies van je wil.
- Door niet zomaar een afspraak te maken en te daten. Nooit een date zonder ouders of leerkrachten, of vriendjes en vriendinnetjes erbij te betrekken!

Directies kunnen aan preventie doen door de "Click safe"-affiche op te hangen (zie www.clicksafe.be). De affiche bevat tips om jonge internetgebruikers te sensibiliseren over het thema. Leraars kunnen aan preventie doen door in de les aandacht te besteden aan zowel de mogelijkheden als aan de risico's van chatten. De leerlingen moeten beseffen dat een openbare chatbox een publieke ruimte is, waar dezelfde regels gelden als in een reële publieke ruimte.

Vragen en antwoorden

Zijn er veilige chatboxen?

Wie op zoek gaat naar chatboxen die honderd procent veilig zijn zal al snel worden teleurgesteld. Op internet kan iedereen zich anders voordoen. Een volwassen chatter kan zich als kind voordoen en omgekeerd. Daar kunnen de chatboxhouders niets tegen doen. Kinderen kunnen wel voldoende vaardigheden aanleren om zich zoveel mogelijk te beschermen.



Wat is de eID?

Je eID is je wettelijke identiteitskaart als Belg. Elke Belg vanaf 12 krijgt gelijdelijk aan de nieuwe elektronische identiteitskaart. Alles wat je met je identiteitskaart kon, kan nu met je eID.

Maar de kids-ID is heel wat meer dan een identiteitsbewijs. Ze bevat een chip waardoor jongeren tussen de 12 en 15 jaar de kaart kunnen gebruiken om veilig te chatten of om zich te identificeren bij internet- en andere diensten. Het resultaat is dat men zich geen zorgen meer hoeft te maken over de ongewenste aanwezigheid van volwassenen die zich voordoen als een leeftijdsgenoot. Behalve de eID, heb je natuurlijk ook een bijhorende kaartlezer nodig, die gebruik van de identiteitskaart voor internettoepassingen mogelijk maakt.

Om te chatten in beveiligde chatrooms, moet je je aanmelden met je eID en je identificeren via je eID-pincode. De eID staat garant voor een ongekennd hoge beveiliging. Ten eerste is het onmogelijk om de eID na te maken. Ten tweede wordt de eID na diefstal of verlies onbruikbaar gemaakt, op dezelfde manier als dat voor een bankkaart gebeurt. Ten derde is



er een extra beveiliging onder de vorm van een pincode (ook zoals bij de bankkaart). Goed om weten is dat er in de beveiligde chatrooms toezicht wordt gehouden door moderatoren. Zij zijn de enige volwassenen die wel kunnen volgen wat er in de chatroom gebeurt.

Je kan veiliger chatten op de volgende plaatsen. Meer zullen er ongetwijfeld volgen:

<http://www.chat.be>

<http://www.skynet.be> via www.kidcity.be

<http://breedband.telenet.be>

<http://www.krey.net/saferchat/>

Meer info over de Kids ID:

<http://www2.dnsmaster.be>

<http://eid.belgium.be/nl/navigation/documents/42993.html>

www.eidsite.be/node/32

www.saferchat.be

Wat is het verschil tussen een gesloten chatbox (Instant Messengers), zoals MSN, Gaim of GoogleTalk en een open chatbox?

MSN is erg populair. MSN is een programma dat het kind op de eigen computer installeert en waarmee het met vriendjes en vriendinnetjes kan chatten. In MSN wordt een contactpersonenlijst aangemaakt. Iedereen die toegevoegd wil worden, zal eerst toestemming moeten krijgen van de ander. Een kind geeft de ander dus toestemming om contact op te nemen via MSN. Een kleine handleiding van MSN vind je op www.i-city.be/manuals/MSN-Messenger.pdf.



Een open chatbox werkt anders. Open chatboxen zijn websites met daarop een chatbox, waar door iedereen gechat kan worden. Er is vooraf geen toestemming nodig. Een populaire open chatbox is bijvoorbeeld www.place.to.be.

Zijn gesloten chatboxen (Instant Messengers) zoals MSN, Gaim of GoogleTalk veiliger dan open chatboxen?

Kinderen kunnen op een gesloten chatbox zelf uitmaken met wie ze chatten. Immers, hij/zij moet toestemming geven aan de ander voor er kan worden gechat. Iemand waarmee het kind geen contact wil hebben, kan geblokkeerd of verwijderd worden. Kinderen blokkeren vaak anderen.

Als ze maar even ruzie hebben, dan wordt de ander 'geblokt' zoals ze het noemen. Open chatboxen hebben de mogelijkheid van blokkeren niet altijd. Er zijn chatboxen waar je andere chatters kunt negeren. Dat wil zeggen dat je alles wat de ander schrijft niet meer kunt lezen.

Kunnen we niet beter kinderen verbieden om te chatten?

Dat is een mogelijkheid, maar kinderen willen erg graag chatten. Ze zullen het op een andere plek doen, waar je als opvoeder geen controle hebt. Liever leren we de kinderen zo veilig mogelijk te chatten en dat, als er iets mis gaat, ze weten wat ze kunnen doen.

Voor kinderen is communicatie heel belangrijk. Vooral bij meisjes zien we dat communicatie op een hoog plan staat. Kinderen (met name jongeren) onderhouden via Instant Messengers hun sociale contacten, en die zijn heel belangrijk voor hen.

Hoort chatten op school thuis?

Er zijn scholen die in hun internetprotocol hebben staan dat chatten niet mag. Er zijn ook scholen die vinden dat chatten mag, als de leerkracht toestemming heeft gegeven. Dit bepaal je als school.

Wat is educatief chatten?

Chatten wordt bovendien door sommige scholen gebruikt in educatieve projecten. Om bijvoorbeeld kinderen in verschillende werelddelen met elkaar in contact te laten komen. Dit wordt regelmatig gebruikt om bijvoorbeeld de Engelse taal te oefenen. Andere mogelijkheid is om chatten juist in te zetten tijdens een project tussen scholen in dezelfde plaats of regio. Dat is bijvoorbeeld het geval geweest bij een verkeersproject, waar kinderen elkaar tips gaven over de verkeerssituaties rond hun scholen.

Een ander gebruik dat minder toegepast wordt, maar wel een optie is, is om kinderen die moeite hebben met schrijven/lezen juist te laten chatten met anderen. Chatten is een leuke bezigheid, die het kind kan stimuleren om op een ontspannen, leuke manier met taal bezig te zijn. (Mits natuurlijk de afspraak dat er in goed Nederlands getypt wordt.)

Welke zijn de Surf Safe veiligheidstips van Childfocus?

1. Ik leg uit aan mijn ouders wat ik doe op het Internet.
2. Ik geef nooit zomaar mijn naam, adres, telefoonnummer of foto aan iemand die ik heb leren kennen via het net, zelfs als deze daar om vraagt.
3. Mijn paswoord is strikt persoonlijk, ik verklap het aan niemand. Het is een beetje als de sleutels van mijn huis: ik geef ze niet aan gelijk wie.
4. Als ik met iemand heb kennis gemaakt via het Internet en “in het echt” wil ontmoeten, overleg ik eerst met mijn ouders.
5. Ik beëindig elke communicatie en ik verwittig mijn ouders van zodra ik informatie ontvang, deelneem aan gesprekken of beelden tegenkom, waarbij ik me ongemakkelijk voel.
6. Ik geloof niet alles wat ik zie en hoor op het Internet; ik leer kritisch zijn.
7. Wanneer ik via het Internet communiceer, blijf ik altijd fatsoenlijk. Ik doe niets dat andere personen kan kwetsen of ongemakkelijk maakt.

Bron: Childfocus (www.childfocus.be)

Hoe zit het met cammen tijdens een chat?

Cammen houdt in dat er gebruik gemaakt wordt van een webcam. De webcam is een klein cameraatje dat op of naast de monitor gezet kan worden. Via MSN bijvoorbeeld kan gebruik gemaakt worden van de webcam. Je kunt elkaar dan zien en zelfs ook horen. Een webcam is niet duur in aanschaf en makkelijk aan te sluiten.

Wil een kind gebruik maken van de webcam? Dan het liefst alleen met anderen die ze al kennen. Bijvoorbeeld kinderen uit de klas, familie of vrienden/vriendinnetjes van sportclub of uit de buurt. Dat neemt niet weg dat anderen alsnog de beelden van de webcam kunnen opnemen en later tegen het kind kunnen gaan gebruiken.

Zo gebeurt het vaak dat webcamsessies worden opgenomen en later gebruikt worden als pestmiddel of chantagemiddel. En zoals meestal het geval is, gebeurt pesten door iemand uit de eigen omgeving. Laat kinderen daarom van te voren bedenken wat ze doen of zeggen tijdens een webcamsessie.

Ze (met name de meisjes) zullen niet de eersten zijn die gevraagd worden om allerlei seksuele handelingen te verrichten voor de webcam of bijvoorbeeld ‘bloot’ te laten zien.

Vaak zijn ouders niet op de hoogte dat er via MSN ook gebruik gemaakt kan worden van de webcam. Het is goed om ouders daarop attent te maken.

Waar kan je kindermisbruik op internet melden?

- **Childfocus**, het Europees Centrum voor Vermiste en Seksueel Uitgebuite Kinderen, verleent sinds 1998 actieve steun aan de opsporing van verdwenen, ontvoerde of seksueel misbruikte kinderen en werkt mee aan de preventie en de bestrijding van kindermisbruik. (www.childfocus.be)
- **Federale Computer Crime Unit (FCCU)** is een politiedienst die zich specialiseert in de strijd tegen computercriminaliteit. De afdeling internetopsporingen ondersteunt de strijd tegen kindermisbruik en kinderpornografie. Die FCCU-afdeling voert opsporingen op het internet en staat daarnaast onder meer in voor het beheer van het Centraal Gerechtelijk Meldpunt op het internet en het geven van vormingen. (<http://www.nedbel.be/internetpolitie.htm>)

Meer weten:

<http://to.be/content/veilig.php>

<http://www.clicksafe.be/>

www.saferchat.be

<http://www.ecops.be/>

www.childfocus.org

<http://users.skynet.be/karendm/>

veilig chatten met de eID

een online meldpunt van de politie

een online meldpunt

een kwisje over veilig chatten

(Zie ook de websitelijst achterin deze leerkrachtenhandleiding.)

Hoofdstuk 4 Blijf lekker buiten

Doel:

- Leerlingen kunnen omschrijven wat computervirussen zijn.
- Leerlingen kunnen omgaan met virusmails.

Te behandelen onderwerpen:

- Uitleg wat een virus is en wat een virus kan aanrichten. Van wie of hoe krijg je virussen?
- Uitleg geven over het kraken van een account. Hoe kan iemand jouw account kraken, wat kun je ertegen doen en hoe kun je het voorkomen?

Gemiddelde tijdsinvestering: 1 lesuur

Wat is ...

Virus = Klein bestand, dat bedoeld is om zich onopgemerkt in andere computers te nestelen. Waarna bestanden op de pc beschadigd kunnen worden of bijvoorbeeld gegevens/bestanden verspreid kunnen worden. Virussen kunnen op vele manier op de pc terechtkomen. Bijvoorbeeld via e-mail, maar ook via het downloaden van bestanden of simpelweg door naar een website te surfen die virussen meegeeft aan een bezoeker.

Evaluatie

Wat hebben we de vorige les gedaan en wat hebben we ervan geleerd? Leg nogmaals uit wat het belang is van een goed wachtwoord.

Opdracht 9

- Titel: Ik krijg geen virus
- Korte inhoud: Je geeft een korte uitleg over virussen. Waar komen virussen vandaan en wat kunnen ze aanrichten? Leg uit dat een virus ook via een diskette van iemand anders op je pc kan komen, of via een zelf gebrande cd, via het downloaden van allerlei bestanden of zelfs door gewoon te surfen op internet.
- Vraag aan de leerlingen of ze op de computer thuis wel eens een virus hebben gehad. Laat de leerlingen uit eigen ervaringen vertellen.

Via het volgende spel kan je laten zien hoe een virus om zich heen kan grijpen.

Benodigdheden: aardappelzetmeel
Betadine of jodium
plastic bekens (1 per leerling en 1 voor uzelf)
theelepels voor iedereen
maatbeker
water
pan
eetlepel
eventueel garde
maatbeker
gasfornuis

Vorbereiding: Je zal voor deze proef aardappelzetmeel moeten koken. Dat kan een dag van tevoren, thuis (in de koelkast twee dagen houdbaar). Vloeistof met daarin aardappelzetmeel zal doorzichtig moeten zijn en dat wordt aardappelzetmeel alleen wanneer je het kookt. Neem twee eetlepels aardappelzetmeel en een beker water en laat dit in een steelpaan onder af en toe roeren op een vuur aan de kook komen. De vloeistof zal nu vrijwel direct helder kleuren. Laat dit mengsel afkoelen onder af en toe roeren. De vloeistof moet eruit zien als behangplaksel. Zet dan voor iedere leerling en voor uzelf een beker met daarin een lepel klaar, gevuld met 50 ml water. Je eigen beker vul jemet de oplossing van aardappelzetmeel en een kleine laag water.

Uitvoering: Het grote moment is daar. Elk lepeltje water uit een bekertje stelt een e-mail voor. De leerlingen en jij gaan elkaar nu een 'e-mail' sturen d.m.v. de lepeltjes water. Je doet vijf lepeltjes water uit je eigen beker in de bekens van vijf leerlingen. Deze leerlingen doen elk weer vijf lepeltjes water in de bekens van vijf medeleerlingen. Zo verder totdat iedereen aan de beurt is geweest. Iedere keer goed doorroeren. Leerlingen mogen zelf weten wie ze een 'e-mail' geven. Wanneer iedereen aan de beurt is geweest, voeg je aan elke beker drie druppels jodium of Betadine toe. Iedereen roert zijn of haar beker door en dan blijkt dat het water in de bekens van de leerlingen en van uzelf paars kleurt. Naar gelang de kleur paars sterker is, is de besmetting erger. Zo gaat het ook met virussen via de mail: hoe donkerder de kleur paars, hoe meer virussen iemand heeft gekregen per mail. Leerlingen kunnen in het werkschrift in een kleurenblok aangeven in welke mate ze virussen hebben opgelopen.

De slotvraag die je kan stellen is of de leerlingen enig idee hebben wie het virus verspreid heeft.

Opdracht 10

Titel:	Informatie zoeken
Leermiddelen:	pc met internetverbinding, pennen
Korte inhoud:	Voor deze opdracht gaan de leerlingen informatie zoeken over virussen. Neem met de leerlingen de websites en/of startpagina's door waar ze kunnen gaan zoeken naar de informatie. In deze opdracht ontdekken de leerlingen dat er straf staat op het verspreiden van virussen aan de hand van het voorbeeld van het Sasservirus dat vele bedrijven schade heeft berokkend. Daarnaast gaan leerlingen bekijken hoeveel virussen er rondwaren op internet en waar je informatie kunt vinden om virussen te bestrijden.

Websites over beveiliging van de computer:

antivirus.startpagina.be/
ictopschool.startpagina.be/
ludit.kuleuven.be/software/virus.html
www.belgium.be/peeceefobie/
http://beveilig.uwpc.info/
www.telenet.be/nl/thuis/internet/veiligheid/anti-virus/index.page (met videofragment)

Antwoorden op de vragen:

- Sven J., een 18-jarige Duitse virusschrijver
- *Hyperlink Virussen* → *Meldingen ontvangen van het BIPT*
- antivirus.startpagina.be
- zie hierboven (*Websites over beveiliging van computers*)

Opdracht 11

Titel:	Downloaden
Leermiddelen:	pennen en een pc met internetverbinding
Korte inhoud:	Lees de probleemstellingen in het werkboek.

Jonas en Muzaffer: Jonas laat aan Muzaffer zien hoe je aan een e-mail zou kunnen zien dat het een virusmail is. De vraag is of de leerlingen dat ook weten. Meerdere antwoorden zijn mogelijk en bij elk antwoord wordt uitleg gegeven.

Laura en Tine: Laura zit met een probleem. Ze heeft tijdens het downloaden van muziek een virus op haar computer gekregen. Laura wil weten hoe je virussen kunt tegenhouden. Een goede virusscanner en het ophalen van updates zijn de juiste antwoorden. Bij elk antwoord wordt een uitleg gegeven.

Extra Opdracht

Titel: Nep

Leermiddelen: pennen en een pc met internetverbinding

Korte inhoud: Nepberichten via e-mail komen regelmatig voor en kunnen gebruikt worden om virussen te verspreiden. In deze opdracht wordt verwezen naar het nepbericht van Kinapolis (website www.adcom.be → t'Is maar ...) dat op 12/02/2004 werd gestuurd. In het bericht staat dat je zowiezo 32 gratis filmtickets krijgt als je enkele mails verstuurt Laat de leerlingen het bericht goed lezen. Laat de leerlingen vertellen hoe zij zien dat het bericht niet echt waar kan zijn.

Je kan met de leerlingen ook andere berichten bekijken op deze website, zoals het nepbericht over het 'bewaarengeltje' van 02/02/2006. Bekijk de berichten en bespreek ze met de leerlingen.

Het nepbericht:

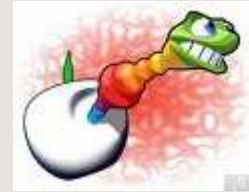
Naam:	Kinapolis hoax
Datum:	12 februari 2004
Eigenschappen:	Subject: kinapolis
	Gewoon verder sturen naar zeven mensen, met een kopie naar info@kinapolis.com en je krijgt 32 gratis filmtickets voor 4 personen.
	Ze doen een actie van Kinapolis via het internet. Het schijnt te werken. Dus... doen!

Achtergrondinformatie bij hoofdstuk 4

Virussen, firewalls en spyware

Virussen

Een virus is een klein bestand, dat bedoeld is om zich onopgemerkt in andere computers te nestelen. Waarna bestanden op de pc beschadigd kunnen worden of bijvoorbeeld gegevens/bestanden verspreid kunnen worden. Virussen kunnen op vele manier op de pc terechtkomen.



Bijvoorbeeld via e-mail, maar ook via het downloaden van bestanden of simpelweg door naar een website te surfen die virussen meegeeft aan een bezoeker.

Het is bijna onmogelijk om nooit een virus binnen te halen. Het is wel mogelijk om een computer zoveel mogelijk te beschermen zodat een virus geen schade aan kan richten op de pc. Ook kinderen halen van alles via internet op. Denk maar aan muziek die zij downloaden of foto's die met een mailtje meekomen. In alle bestanden, zoals muziek en foto's, kunnen virussen zitten. Daar kan de ontvanger niets aan doen, het gebeurt iedereen.

Hoe gaan virussen te werk?

De definitie van een virus zoals hierboven gegeven laat al zien hoe onvoorspelbaar de werking is. Met enige regelmaat wordt er melding gemaakt via de media van een gevaarlijk virus. Vooral grote bedrijven zijn het slachtoffer van deze aanvallen. Maar ook particulieren kunnen natuurlijk belaagd worden door virussen. Het is daarom belangrijk om altijd een virusscanner te installeren op de pc. Informatie over virussen en virusscanners kan je vinden op www.antivirus.startpagina.be.

Titel:
W32.Mixor.q@mm (alias W32.Numar)
Datum:
31 december 2006
Type:
High risk mailing
Bericht:
Zwolle, 31 december 2006
Beste abonnee van VirusAlert,
Een nieuwe internetworm is op dit moment zeer actief in de Benelux, het vermomt zich als een nieuwjaarsgroet, maar gebruikt ook teksten als "Bush en Poetin overleden" etc. In de e-mail wordt gevraagd om het bijlagebestand te openen. Doet dat niet!
Open je dit .exe bestand dan wordt je systeem met dit virus besmet. Na infectie installeert het een trojan waardoor de aanvaller controle over jou systeem kan uitoefenen. Ook verstuurt het zich vervolgens vanaf jou besmette systeem door naar alle contacten in het aanwezige adressenboek.
Meer informatie over dit virus, kijk op de website van VirusAlert: http://www.virusalert.nl/?show=virus&id=1719&name=W32.Mixor.q@mm%20(Numar)

Risico's

Een virus wordt meegestuurd met een e-mail of een ander bestand

Als je op de computer een virusscanner hebt geïnstalleerd (en up-to-date heeft gehouden) wordt het virus in quarantaine geplaatst en/of verwijderd.

Een virus heeft de computer al besmet

Je kan te laat zijn. Een virus heeft de pc al besmet. Dat kan je bijvoorbeeld zien omdat je voor de eerste maal de virusscanner hebt geïnstalleerd, die je hele systeem scant op virussen. Of je virusscanner is niet up-to-date en beschermt niet tegen de nieuwste virussen.

Kinderen, ouders of jij merkt/merken dat er iets mis is met de computer

Een virus kan ervoor zorgen dat de pc anders reageert dan de bedoeling is. Bijvoorbeeld: de pc loopt steeds vast of de internetverbinding wordt heel erg traag. Het kan zijn dat een virus actief is op de pc.

Oplossingen

Op elke computer hoort een goed werkende virusscanner te zitten. Goed werkend houdt in:

- een virusscanner die voldoende virussen herkent (en zijn werk goed doet);
- een virusscanner die zichzelf regelmatig informeert over de nieuwste virussen (updates ophaalt via het internet).

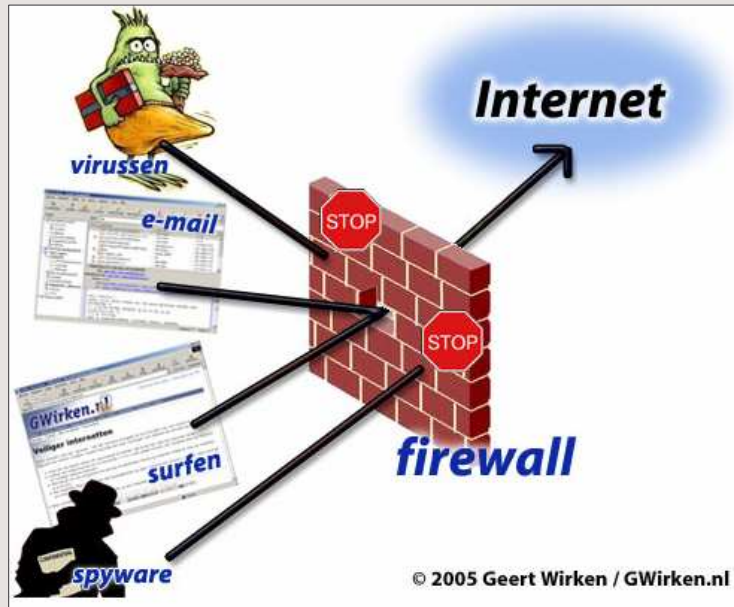
Voorbeelden van online virusscanners: Panda (www.panadasoftware.com), Kapersky (www.kaspersky.com).

Voorbeeld van een virusscanner: AVG (free.grisoft.com)

Firewalls

Een firewall is een beveiliging tussen het externe (internet) en het interne netwerk (LAN), dat probeert te voorkomen dat onbevoegden toegang krijgen tot het interne netwerk. Men kan wel van binnen naar buiten gaan, maar niet andersom zonder toestemming.

Als de computer een constante verbinding heeft met internet, bijvoorbeeld omdat je aangesloten bent via de



kabel of via een adsl-verbinding, dan loop je meer risico. Degenen die proberen in andere computers binnen te komen, worden hackers genoemd. We bevelen aan om op de computer een firewall te zetten. Een firewall is gratis te downloaden. Een voorbeeld van een firewall die gratis is en goed uit tests van gebruikersorganisaties komt: ZoneAlarm (www.zonelabs.com).

Spyware

Bij het surfen kunnen op de computer programmaatjes achtergelaten worden die de bedoeling hebben het surfgedrag van de gebruiker te volgen of, erger nog, gegevens van de gebruiker te achterhalen. Deze programmaatjes heten spyware. Ze volgen bijvoorbeeld het surfgedrag van de gebruiker, maar er is ook spyware die gegevens proberen te achterhalen en bijvoorbeeld accountgegevens opslaan. Ook al ben je geen grote gebruiker van internet, toch is het aan te raden om wekelijks de spyware te verwijderen. Er bestaat veel software om dit te doen. Er zijn gratis programma's beschikbaar. Hieronder vind je de websites om deze te downloaden en te gebruiken.

Anti-spyware programma's:

<http://www.lavasoftusa.com/software/adaware/> (anti spyware software)

<http://www.safer-networking.org/> (spybot)

Meer info op

<http://ludit.kuleuven.be/software/beveiliging/spyware.html>

<http://www.nedbel.be/anti-spyware.htm>

Spyware killer: € 7,99



Download

Samenvatting: Spoor spyware programma's op en verwijder ze! Spyware killer is een programma dat allerlei soorten spyware programma's opspoor en ze verwijderd!

Grootte: +/- 35 MB

Taal: Nederlands

Bestandstype: .exe

Video formaat: 0x0

Systeemeisen: pentium 500 mhz, 64 mb ram, geluidskaart, cd recorder (optioneel), 1 gb vrije harde schijf ruimte, ms windows 98/me/2000/xp

Kijkwijzer: 

Vragen en antwoorden

Is het mogelijk om virus-vrij te surfen en e-mailen?

Helaas zijn er erg veel virussen op internet. Het is bijna niet meer mogelijk om 'zomaar' en zonder kleerscheuren (lees: virussen) te internetten of te e-mailen. Ga ervan uit dat een goede virusscanner een must is.

Als ik internet heb met een telefoonlijn, loop ik dan ook het risico te worden 'gehackt'?

Wie geen constante verbinding met internet heeft, loopt minder risico. Wie inbelt via een telefoonlijn krijgt automatisch steeds een ander ip-adres toegewezen. Dit is heel simpel gezegd het nummer dat je computer toegewezen krijgt. Daarnaast ben je niet continu verbonden met internet. Daardoor loop je minder risico. ADSL of kabelaansluiting heeft tot gevolg dat er verbinding is zodra de computer aangezet wordt. Je computer heeft in dat geval een vast ip-nummer. Helaas is niemand gevrijwaard van inbraakpogingen. Een beginnende hacker zal een willekeurig ip-adres proberen om in te breken. Bij particulieren is dat meestal veel eenvoudiger dan bij bedrijven, die hun netwerk over het algemeen goed beveiligd hebben. Zorg dus altijd, welke verbinding je ook hebt, voor goede bescherming.

Mijn leerlingen zeggen te zijn gehackt. Een jongen had het erover dat zijn MSN-adres is gehackt. Wat bedoelt hij dan?

We denken dat de kinderen uit je groep ervaren dat er iemand anders via hun e-mailadres post verstuurt of leest. Kennelijk is iemand anders achter het wachtwoord gekomen van het e-mailadres van deze leerlingen. (Dit geldt overigens voor alle accounts die kinderen hebben, bijvoorbeeld op Kidcity, profielwebsite, MSN of e-mail). Het is niet het 'hacken' zoals wij dit in dit hoofdstuk bedoelen, maar de kinderen vatten dit kennelijk wel zo op.

Eénmaal gehacked is het moeilijk om het account weer terug te krijgen. De hacker heeft waarschijnlijk het wachtwoord veranderd. Advies is om iedereen te laten weten dat het account gehacked is, zodat anderen het weten en niet vreemd opkijken van rare berichten. Advies aan alle leerlingen (en ook volwassenen), zorg voor een goed wachtwoord en houd het geheim.

Hoofdstuk 5 Gewoon doen of niet?

Doel:

- Leerlingen zijn zich bewust van banners/pop-ups die leiden naar ongewenste sites.
- Leerlingen kunnen omgaan met uitnodigende banners op internet. Leerlingen zijn zich bewust dat doorstuurmailtjes niet waarheidsgetrouw zijn.
- Leerlingen kunnen omgaan met e-mail die niet vertrouwd is.

Te behandelen onderwerpen:

- Wat zijn banners en pop-ups?
- Waarom staat er reclame op websites?
- Kun je zomaar op een site komen die niet geschikt is voor kinderen?
- Wat doe je als je op een dergelijke site terecht komt?
- Herhalen dat niet alles wat op internet staat ook waar hoeft te zijn.
- Kosten van handelen op internet (spelletjes, per ongeluk iets bestellen).

Gemiddelde tijdsinvestering: 1 lesuur

Evaluatie

Wat hebben we de vorige les gedaan en wat hebben we ervan geleerd?

Opdracht 12

- Titel:** Reclame
- Leermiddelen:** pennen en pc met internetverbinding
- Korte inhoud:** Internet staat boordevol reclame. Deze opdracht is bedoeld om kinderen bewust te maken van deze reclame, dat ze kritisch leren kijken naar reclame en dat ze weten waarom reclame op een site staat. Je bespreekt met de leerlingen op welke websites veel reclame en popups te zien zijn. Je legt uit wat het verschil is tussen een reclamebanner en een pop-up.



De leerlingen beantwoorden de vragen in het werkschrift. Ze gaan op zoek naar drie websites (dit kunnen hun eigen favoriete websites zijn) en geven aan welke en hoeveel reclamebanners en pop-ups zij tegenkomen. Je kan bij deze opdracht ook enkele van deze webpagina's printen. Deze prints kunnen klassikaal worden besproken om bijvoorbeeld te kijken wat voor beloftes in reclame worden gedaan en wat deze voor consequenties kunnen hebben op financieel gebied.



Opdracht 13

Titel: Help
Leermiddelen: pennen
Korte inhoud: In deze opdracht maken de vier kinderen in de cursus verschillende gebeurtenissen mee. Aan de leerlingen wordt gevraagd wat de karakters het beste kunnen doen in een bepaalde situatie.

- Leg uit wat Jonas zou kunnen doen nu hij een virus op zijn computer heeft. Jonas zou alsnog een virusscanner moeten gebruiken om het virus te verwijderen. Bespreek nogmaals hoe je je tegen virussen kan wapenen.

- Leg uit wat Muzaffer zou kunnen doen om in het vervolg de hoogte van de telefoonrekening van zijn ouders niet meer te laten afhangen van de spelletjes die hij aanklikt op internet. Natuurlijk moet - Muzaffer zelf goed opletten bij het aanklikken van betaalsites. Zijn ouders zouden de inbelnummers van deze spelletjes (0900 nummers) door de telefoonprovider kunnen laten blokkeren.

- Leg uit wat Laura gedaan heeft en waar ze niet op gelet heeft; Laura heeft er niet op gelet of ze bij het invullen van het formulier iets ging bestellen, waarvoor ze moest betalen.

- Leg uit waar Tine op bedacht moet zijn als ze haar e-mailadres op een chatbox heeft doorgegeven en haar nu de vraag wordt gesteld of ze een foto van zichzelf op wil sturen. Als ze dit doet geeft ze veel privé-gegevens aan een onbekende vrij. De foto en het e-mailadres zouden bijvoorbeeld door de ander misbruikt en op een website gepubliceerd kunnen worden.

Opdracht 14

Titel: Websites voor volwassenen
Leermiddelen: pennen
Korte inhoud: Sommige websites zijn niet voor kinderen bestemd, maar voor volwassenen. In de opdracht gaan we in op deze websites. Je kan zelf bepalen over welke onderwerpen gepraat wordt en in hoeverre je hierop ingaat.
Het kan zijn dat kinderen alleen met voorbeelden komen van websites die voor volwassenen zijn, maar waar niets mis mee is. Bijvoorbeeld websites over vakanties, sport, de beurs, musea e.d.
Er zijn ook websites die voor volwassenen bestemd zijn, maar door veel volwassenen niet gewenst zijn. Bijvoorbeeld websites met geweld, discriminatie, porno. Denk bijvoorbeeld aan webadressen als 'www.poes.be' of een zoekopdracht in een zoekmachine die websites oplevert die volgens de kinderen helemaal niets met het zoekwoord te maken hebben. Met name woorden die voor meerdere uitleg vatbaar zijn, waar kinderen nog geen notie van hebben.
Leg de leerlingen uit dat sommige woorden een dubbele betekenis hebben en daarom ook gebruikt worden in deze websites. Belangrijk is dat de leerlingen weten dat het niet hun 'schuld' hoeft te zijn dat ze op ongewenste sites terecht komen. (Alhoewel oudere leerlingen natuurlijk wel nieuwsgierig worden en wel degelijk met opzet bepaalde websites gaan bezoeken.)

Extra opdrachten

Titel: Reken maar uit
Leermiddelen: pennen
Korte inhoud: Voor het gebruik van sommige websites of spelletjes moet betaald worden. Dit kan ongemerkt gaan d.m.v. een dialer (programmaatje dat verbinding maakt met een duur 0900-nummer) of leerlingen krijgen een pop-up te zien, waarin staat dat ze een 0900-nummer moeten bellen om het spelletje te kunnen spelen. Uiteraard mogen ze dan niet ophangen zolang ze aan het spelen zijn, aldus de website.
Kinderen zien niet direct de kosten die daarmee gepaard gaan. Het is belangrijk dat leerlingen zich bewust worden van de kosten. Je kan deze opdracht eventueel zelf uitbreiden met meerdere rekenopdrachten.

Meer info op
mineco.fgov.be/protection_consumer/fraud_prevention/folders/Telephone_nl.pdf

Antwoord:
- 36 euro
- 6 maanden

Titel: Zoek de website
Leermiddelen: pennen
Korte inhoud: Sommige websites staan bol van allerlei reclame. Dit kunnen banners zijn, maar ook ongevraagde pop-ups. Bedoeling van de opdracht is de leerlingen te laten inzien dat ze ongevraagd overstelpt worden met reclame. Maak de leerlingen bewust van het feit dat ze kritisch moeten omgaan met de reclame, en dat het de enige bedoeling is om hen in de val te lokken ... namelijk het product te kopen.

Antwoord:
- 2 banners (nl. Axa, Helpen stoppen met roken)
- 1 pop-up (Fortuneo)

Achtergrondinformatie bij hoofdstuk 5

Ongewenste sites

Wat zijn ongewenste sites?



Ongewenst is voor iedereen weer anders. Ook voor kinderen. De één vindt iets heel eng, de ander vindt het leuk. Dat geldt ook voor volwassenen. Als we het in het lesmateriaal over ongewenste sites hebben, dan praten we over sites met porno, seks(ualiteit), geweld, discriminatie, racisme e.d.

Valt het surfen naar ongewenste sites te voorkomen?

Wie op internet surft, komt nu eenmaal ongewenste websites tegen. De enige manier om het voor een groot deel uit te sluiten, is het instellen van een zeer beperkende inhoudsfilter. Deze mogelijkheid wordt hieronder besproken. Nadeel hiervan is dat kinderen op een andere plaats dan school wel ongewenste websites kunnen zien, en niet weten hoe ermee om te gaan.

Voor kinderen van de eerste graad van het basisonderwijs (en eventueel eerste graad van het secundair onderwijs) kan het raadzaam zijn te werken met een inhoudsfilter. Kinderen in het secundair hebben al meer inzicht en voor hen kan het leren omgaan met ongewenste websites zonder inhoudsfilter een voordeel hebben. Uiteindelijk zullen ze waar dan ook in contact komen met ongewenste websites en moeten leren hoe ze daarmee om moeten gaan. Je kan het vergelijken met een weerbaarheidstraining.

Oplossingen

Kinderen leren omgaan met de informatie op internet is de beste manier om hen voor te bereiden en weerbaar te maken wanneer ze zelfstandig aan de slag gaan met internet.

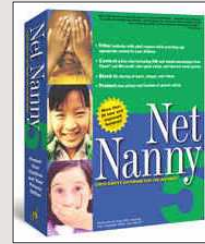
Je kan het vergelijken met het verkeer. De kinderen leren omgaan met het verkeer en leren weerbaar te zijn in het dagelijks leven. Dit geldt ook voor het internetten. Ook weten we allemaal, dat kinderen misschien wel weten hoe iets wel/niet moet, maar of ze het ook doen is natuurlijk een andere vraag. Als opvoeders/leerkrachten kunnen we er alleen voor zorgen dat ze de basis meekrijgen.

- Op je **standaardbrowser** kan je een filter activeren die bepaalde sites blokkeert.

Bij de eigenschappen van 'Internet Explorer' en 'Netscape' kan je met een klik de internetbeperkingen instellen. Deze filtering houdt een groot aantal sites tegen, maar een hoop adressen glippen door de mazen van het net. De restricties zijn bovendien alleen van toepassing op webpagina's. Ook e-mail, chat en nieuwsgroepen kunnen immers ongewenste beelden en informatie geven.



- Scholen kunnen ook **software** aanschaffen om software te filteren. *Netnanny* en *Cyberpatrol* blokkeren tijdens het surfen websites waar bepaalde woorden op voorkomen. Deze software kan ook werken op basis van een databank met een zwarte lijst (blacklist) van webadressen of websites blokkeren die niet behoren tot een witte lijst (white list) van sites die kindvriendelijk zijn. Bovendien screenen sommige filters ook e-mail en nieuwsgroepen.



Filterprogramma's kunnen ook informatie tegenhouden die informatief en/of educatief is. Zo blijkt het zoeken van medische inhoud dikwijls onmogelijk.

- Een andere mogelijkheid is om te werken met **kinderbrowsers**. Deze browsers werken op basis van een beperkt aantal voorgekauwde sites. Het is een uitstekende aanpak voor de allerkleinsten die hun eerste stappen op internet zetten, maar oudere kinderen zullen al snel gefrustreerd geraken door de beperkingen.
- Leraars in het lager onderwijs kunnen zelf een '**zandbak** in cyberspace' opbouwen. Hierbij legt men op een internetpagina (aan pagina van de school) een bibliotheek aan met websites (links). De leerlingen werken op die manier in een afgeschermd leeromgeving.

Bijkomende informatie vind je op

www.ictopschool.net/infrastructuur/publicaties/uitgaven/filter/index.html

<http://onderwijs.vlaanderen.be/publicaties/eDocs/pdf/145.pdf>

Reclame op internet

Websites staan vaak boordevol reclame en pop-ups. De redenen om reclame op een website te plaatsen kunnen zijn:

- er wordt geld verdiend aan de website;
- er wordt geld verdiend aan het verkopen van producten via de website;
- reclamebanners worden onderling geruild om meer bezoekers naar de site te trekken.

Veel websites zijn afhankelijk van reclame-inkomsten. Maar een website is alleen interessant voor adverteerders als deze veel bezocht wordt. Zonder deze reclame zouden er veel minder en vooral actuele websites zijn of moeten website-eigenaren elders inkomsten zien te genereren.

The screenshot shows a news website layout with several elements:

- Top Left:** News snippet: "Minister van Sociale Zaken Rudy Demotte heeft woensdag gezegd dat hij niet van plan is ooit nog b..."
- Top Middle:** News snippet: "het geweld dat in Frankrijk uitbrak na de verkiezing van Nicolas Sarkozy tot president duurt voor..."
- Top Right:** "KRANTEN KLAS" logo.
- Center:** Large advertisement for a Fiat Panda with the text "WIN HIER EEN FIAT PANDA" and the hbvl.be logo.
- Right Side:** "LAAD HIER UW FOTO'S OP" button and a "Charmeoffensief bij Dexia tot 6 juni 2007" advertisement.
- Bottom Right:** "Dossiers" section with links: JM Dedecker, Uitbreiding EU, Verkeersveiligheid, Irak, Overgewicht.

Vragen en antwoorden

Als onze school een inhoudsfilter zou gebruiken, zijn onze leerlingen dan altijd beschermd tegen ongewenste websites?

Zoals ieder technisch hulpmiddel is ook een inhoudsfilter nooit voor honderd procent afdoende. Kinderen zijn daarbij ook nog eens erg slim, en vinden altijd manieren om het filter te omzeilen. Een inhoudsfilter zorgt ervoor dat de meeste ongewenste websites niet getoond worden. Aangezien er op internet dagelijks honderden nieuwe websites bijkomen is het moeilijk om de lijst volledig up-to-date te houden. Al doen de aanbieders natuurlijk wel hun best.

Een inhoudsfilter met alleen white-listing (alleen websites in die lijst kunnen worden bezocht) is nog wel de meest afgeschermd manier van internetten. Nadeel is wel dat wanneer jij of je leerlingen een andere website willen bezoeken dan in de lijst staat, de website dus niet getoond zal worden.

Onze school heeft geen inhoudsfilter, betekent het dan dat onze leerlingen niet beschermd zijn tegen ongewenste websites?

Iedere school probeert haar leerlingen een zo veilig mogelijke omgeving te bieden, ook op het gebied van internet. Sommige scholen kiezen voor een gefilterd internet, sommige scholen niet. Deze keuze heeft ook te maken met de identiteit van de school en de opvattingen die er binnen de school bestaan om om te gaan met het leer- en ontwikkelingsproces van de leerlingen. We bevelen aan om als school te kijken naar hoe je leerlingen omgaan met de risico's van internetgebruik.

Hoofdstuk 6 Digitaal pesten

Doel:

- Leerlingen zijn zich bewust dat pesten niet kan.
- Leerlingen kunnen omgaan met pestmail.
- Leerlingen kunnen omgaan met vervelende chatters.
- Leerlingen zijn zich bewust dat het kraken van een e-mail/MSN-account niet mag.
- Leerlingen zijn zich bewust dat kraken van een account ook pesten is.
- Leerlingen zijn zich bewust van de noodzaak van een goed wachtwoord.

Te behandelen onderwerpen:

- Wat zijn pestmailtjes?
- Wat moet je doen als je pestmailtjes krijgt? Wat vind jij van vervelende chatters?
- Wat moet je doen als er een vervelende chatter op je chatbox zit?
- Wat moet je doen als je iemand hebt toegelaten op je MSN, die opeens allerlei rare vragen gaat stellen en misschien ook nog wel foto's van je wil hebben?
- Hoe kun je iemand blokkeren in mail/chat/MSN? Wie schakel je in als je gepest wordt?
- Pas op met roddelen per e-mail.

Gemiddelde tijdsinvestering: 1 lesuur

Evaluatie

Wat hebben de leerlingen in de voorgaande lessen geleerd? Bespreek nogmaals wat je zou kunnen doen wanneer de leerlingen op sites terechtkomen waar ze in eerste instantie helemaal niet naar op zoek waren.

Benadruk dat je altijd naar ouders of leerkrachten toe kunt gaan om nare sites te melden en ze daarna weg te klikken.

Opdracht 15

Titel:	Wat is pesten en wat niet?
Leermiddelen:	pennen
Korte inhoud:	Bespreek met de leerlingen wat pesten is. Wat voor de één pesten is, kan voor de ander een grapje zijn. Waarom vinden mensen dit zo verschillend? Wat is het verschil tussen pesten op de speelplaats en pesten in bijvoorbeeld een chatbox? Waarom is de ene e-mail wel een pestmail en de andere niet? Je legt uit dat het te maken heeft met de anonimiteit die je je kunt aanmeten wanneer je je beweegt op internet. Dat de impact die pesten heeft per persoon anders is, omdat de gevoelens en ook het zelfbeeld per persoon verschillen; een pesterij zal voor de één confronterender zijn dan voor de ander. Pesten via internet heeft vaak een grotere impact. Tenslotte kan een e-mail of foto met één druk op de knop naar tientallen anderen gestuurd worden. Wat ook vaak voorkomt is dat pesters anderen oproepen om één persoon te pesten. Het slachtoffer wordt bedolven onder pestmail/scheldpartijen op MSN of wordt 'te grazen' genomen in Kidcity.

De vier personages van de cursus hebben een e-mail gekregen waarbij de leerlingen kunnen aangeven of ze het een pestmail vinden, dat ze het niet weten of dat het gewoon een leuke mail is. Je bespreekt met de leerlingen of dit pesten is of niet. Wat natuurlijk voor de één een grapje is, is voor de ander pesten.

Antwoorden:

E-mail Muzaffer is een pestmail. Dit kun je zien aan het bericht dat niet echt leuk is, maar vooral ook aan de emoticons die eronder staan.

E-mail Tine is een grapje. Maar Tine kan het ook opvatten als pesterij. Het ligt eraan wie de e-mail gestuurd heeft. Is het een vriendin waarmee ze altijd veel lol heeft, dan is het waarschijnlijk als geintje bedoeld.

E-mail Jonas is een pestmail. Iemand is niet blij met Jonas. Het lijkt erop dat iemand jaloers op hem is en dreigt zijn MSN te hacken. De emoticons die eronder staan laten zien dat de pester het meent

E-mail Laura is een geintje. Maar ook dit geintje kun je op verschillende manieren opvatten. De emoticons onderaan het bericht vertellen dat het niet kwaad bedoeld is. Maar zou Laura haar mp3 speler meenemen naar school?

Opdracht 16

Titel:

Is digitaal pesten anders dan 'gewoon' pesten?

Leermiddelen:

pennen en pc met internetverbinding

Korte inhoud:

Bespreek met de leerlingen nogmaals het verschil tussen pesten en digitaal pesten. Vraag of ze ermee te maken hebben gehad. Leerlingen gaan op internet op zoek naar websites met informatie over digitaal pesten.

Er worden diverse websites genoemd waar tips te vinden zijn voor kinderen.

De leerlingen vormen groepjes van vier. Ze surfen naar de websites met informatie en beantwoorden ieder voor zich de vragen in het werkschrift.

Hebben ze de vragen beantwoord, dan gaan ze in het groepje hun antwoorden vergelijken.

Ze bespreken wat zij vinden van de tips die ze gevonden hebben en welke oplossingen ze bedacht hebben.

Je kan daarna de tips en oplossingen klassikaal bespreken.

Opdracht 17

Titel: Ga toch weg
Leermiddelen: pennen
Korte inhoud: Leerlingen zien in het werkschrift de personages die alle vier in de chatbox iets meemaken met een chatter. Ieder karakter lost dat op geheel eigen wijze op. De leerlingen kunnen via meerkeuze-antwoorden aangeven wat ze van de oplossing vinden die het karakter heeft gekozen.

Antwoorden:
Muzaffer heeft het goed opgelost
Tine heeft het niet goed opgelost, maar doet mee met het schelden en zorgt er dus voor dat het maar door blijft gaan.
Laura heeft het goed opgelost. Nog beter zou zijn als ze daarna gewoon weg gaat uit de chatbox.
Jonas heeft het goed opgelost. Hij heeft er iemand bijgehaald om mee te kijken en samen hebben ze actie ondernomen.

Extra opdrachten

Titel: Tips Top Tien
Leermiddelen: pennen, pc met internetverbinding
Korte inhoud: Leerlingen zijn al op zoek gegaan naar informatie over digitaal pesten en hebben als het goed is in groepjes en klassikaal gepraat over het voorkomen van digitaal pesten en oplossingen. In deze opdracht gaan ze hun eigen Tips Top Tien samenstellen. De tips kunnen betrekking hebben op:
- het voorkomen van digitaal pesten;
- wat te doen als iemand digitaal gepest wordt;
- oplossingen tegen digitaal pesten.
Je kan deze tips klassikaal bespreken en wellicht één klassikale Tips Top Tien samenstellen en opnemen in het pestprotocol van de school.

Titel: Journalist
Leermiddelen: pennen en papier
Korte inhoud: Leerlingen gaan bij deze opdracht vragen stellen aan kinderen en volwassenen om erachter te komen of digitaal pesten een bekend thema is bij deze groepen. De leerlingen nemen met vier vragen een kort interview af.

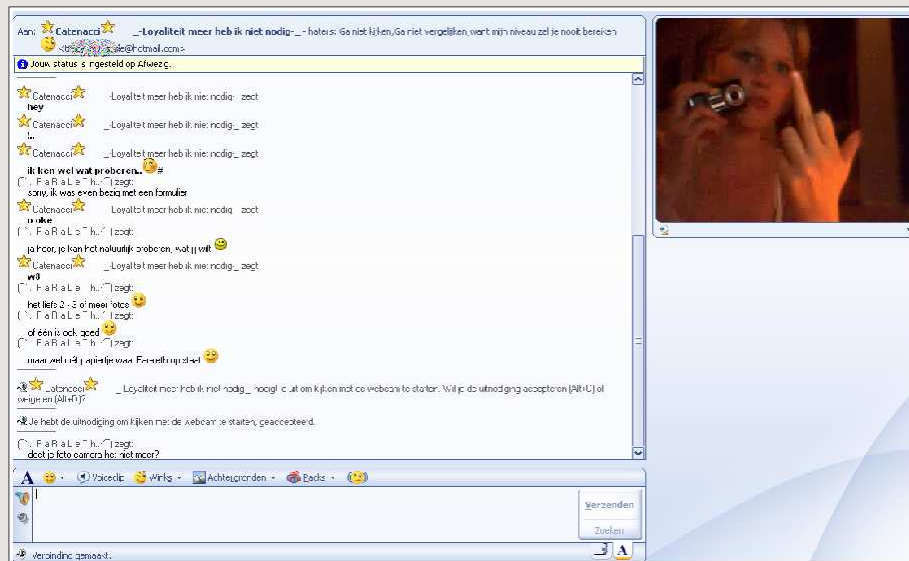
De vragen zijn: Weet je wat digitaal pesten is?
Kan je voorbeelden noemen van hoe dit gebeurt? Via e-mail? Via MSN of een chat?
Ken je iemand die digitaal gepest is?
Wat vind je ervan dat mensen elkaar pesten via internet? Hoe denk je dat het pesten kan stoppen?

Titel: Jouw pestprotocol
Leermiddelen: pennen en papier
Korte inhoud: Leerlingen lezen eerst individueel het stukje pestprotocol in hun oefenboek. Dat is een fragment uit http://www.geocities.com/juf_online/klassen.html
Aan de hand van dit protocol zien ze in dat pesten veel meer is dan alleen de ander voor de gek houden.
Laat de leerlingen vervolgens, eventueel in groepjes, nadenken over zaken die ontbreken in het protocol. Geef hen tips, nl. hoe ga de regels controleren, wat doe je als iemand zich niet aan de regels houdt, hoe pak je het aan als iemand wordt gepest, enz.

Achtergrondinformatie bij hoofdstuk 6

Pesten

Wat is pesten via internet?



Misschien kan je je er geen voorstelling van maken, maar het pesten op de speelplaats heeft zich uitgebreid tot andere communicatiemogelijkheden van kinderen. Dus ook via internet. Kinderen pesten elkaar door e-mail te sturen, op MSN te schelden/dreigen, account te kraken, foto's van iemand online te zetten of bijvoorbeeld berichten over iemand naar een grote groep kinderen te sturen. Op de speelplaats weet een gepest kind in elk geval wie de pester is. Met digitaal pesten kan dat anders zijn.

Al is de pester vaak wel iemand uit de eigen omgeving. Een bijkomend nadeel is dat met digitaal pesten de tekst op het scherm blijft staan. Een e-mail kun je blijven lezen, een bericht dat op internet is gezet krijg je er niet zomaar vanaf. Je hebt als slachtoffer helemaal geen controle meer over wat er gebeurt, nog minder dan met pesten op het schoolplein.

Risico's

Er zijn allerlei manieren om via internet te pesten en te treiteren. Een aantal voorbeelden:

- pesten via e-mail
- pesten via chat/MSN
- pesten via profielwebsite
- pesten door hacken van accounts
- pesten door foto's rond te sturen
- webcamsessies opnemen en doorsturen naar anderen of gebruiken als chantagemiddel

Je moet bedenken dat alle mogelijkheden die internet biedt aangegrepen kunnen worden om iemand te pesten en zelfs te bedreigen.

Uit onderzoeken blijkt dat kinderen die in het dagelijks leven gepest worden of vaak het slachtoffer zijn van plagerijen, ook op internet het meest gepest worden. Het digitaal gepest worden komt er vaak nog eens bovenop.

Oplossingen

Het allerbelangrijkste is dat een kind erover kan praten met ouders en/of leerkracht. Een klein pesterijtje kan een kind zelf misschien nog oplossen, maar als het vaak voorkomt lukt dat niet meer. Leerkrachten kunnen met de leerlingen bespreekbaar maken waar de grens ligt tussen plagen en pesten. Als cyberpesten daarbij ter sprake komt, kan een leraar duidelijk maken dat pesterijen via sms en e-mail minstens even hard aankomen als “gewone” pesterijen. Leerlingen moeten ook beseffen dat een gsm-nummer en een e-mailadres tot de privé-sfeer behoren en dat je die gegevens niet zomaar te grabbel gooit.

Praten is belangrijk. Maar vooral ook is het van belang dat een volwassene zich realiseert dat digitaal pesten meer impact heeft dan ‘gewoon’ pesten. Daarnaast moeten volwassenen zich realiseren dat digitaal pesten op allerlei manieren kan voorkomen en het dus niet weggewuifd wordt dat het allemaal wel mee zal vallen.

Er zijn diverse mogelijkheden om het pesten te stoppen.

- **Blokkeren** van een e-mailadres, dit kan via e-mailprogramma's en ook in veel webmailprogramma's is deze mogelijkheid aanwezig. Selecteer bij 'MS Outlook' het bericht van de afzender die je wil blokkeren, en klik vervolgens in het menu 'Bericht' op 'Afzender blokkeren'.
- **Bewaren** van de e-mails (originele versie)
- Blokkeren of **verwijderen** van iemand in de MSN. In chatboxen is soms de mogelijkheid om een chatter te negeren.
- Bij pesten of ongewenst gedrag in **chatboxen** kan de chatboxhouder op de hoogte worden gesteld. Wordt iemand gepest in een open chatbox, dan kan die persoon het beste de chatbox verlaten en een leukere chatbox opzoeken.
- Wordt iemand gepest via een **profiel**, dan kan de website-eigenaar op de hoogte worden gebracht. Vaak is er een redactie aanwezig die berichten op profielen kan verwijderen en/of gebruikers een waarschuwing kan sturen.

The screenshot shows a Windows Live Spaces profile for a user named 'maxime'. The profile includes a photo gallery, a bio, and a blog post. The bio states: 'Wanna be Photomodel'. The blog post, dated 16/02/07, is titled 'maxime's news' and contains the following text: 'ey mensen alles kids met jullie met mij wel tot nu toe. woon reeds een jaar en enkele maanden alleen in omgeving CHARLEROI goed nieuws ik en mijn vriend ; hij wil nederlands leren dus gaan we hoogwaarschijnlijk naar limburg komen zal dan omgeving bree gaan wonnen samen met mn vriend en hopelijk tot binnekort greetz M a x i m e ps: ik weet dat ik nogal veel heb gezecht dat ik binne kort met een nieuwe agentschap zou werken dat mijn site bijna af is het zit namelijk zou d site waren ze er mee bezig maar omstandigheden gaat het niet door en moet ht op een andeemanier zien te krijgen en het agentschap gaat ook niet door want hen wat hij gekomen'.

- Het hacken van accounts kan voorkomen worden door een goed wachtwoord en uiteraard het geheim houden van dat wachtwoord. Is een account gehacked, laat dan zo snel mogelijk iedereen in je adresboek weten dat het account gehacked is. Het account terugkrijgen is niet altijd even eenvoudig. Je moet kunnen bewijzen dat het account oorspronkelijk van jou was. Het beste is om een nieuw account aan te maken en daarvan de gegevens goed geheim te houden.
- Tegen het doorsturen van foto's of bijvoorbeeld webcamsessies is vaak weinig te doen. Het kind kan hooguit een volwassene in vertrouwen nemen en de pester aanspreken op zijn of haar gedrag. Dit kan bijvoorbeeld door de ouders van de

pester op de hoogte te stellen. Circuleren de foto's/webcamsessies op internet, dan kan de website-eigenaar gevraagd worden deze te verwijderen.

Als het pesten blijft duren, moet er een bepaalde expertise worden voorzien. Kinderen die het slachtoffer worden van elektronische pesterijen moeten terecht kunnen bij een leraar of bij een vertrouwenspersoon en het Centrum voor Leerlingenbegeleiding waarmee de school verbonden is. Het Steunpunt Grensoverschrijdend Gedrag op School is het aanspreekpunt bij uitstek voor pesten en ongewenst seksueel gedrag. De vzw Limits behandelt in opdracht van de minister van Onderwijs pestklachten in het onderwijs. Zij biedt opvang en steun aan slachtoffers en advies aan scholen.

Info op www.limits.be

Vragen en antwoorden

Wat is het verschil tussen het 'gewone' pesten en het pesten via internet of mobieltjes?

Het grote verschil voor kinderen is de anonimiteit en het gemak waarmee wordt gepest. Een kind kan heel gemakkelijk een e-mail versturen en de ander niet in de ogen hoeven te kijken. Vervelende e-mails of berichten komen heel hard over als het zwart op wit staat. Een kind kan het bericht blijven lezen. Daarnaast is, zoals eerder besproken, de mogelijkheid om grootschalig te pesten veel gemakkelijker via digitale media dan 'gewoon' pesten op het schoolplein. Met één druk op de knop kunnen vele mensen tegelijk bereikt worden.

In 2006 heeft het viWTA een onderzoek gedaan naar pestgedrag. De resultaten zijn te lezen in het rapport: 'Cyberpesten bij jongeren in Vlaanderen'. Het hele verslag kun je downloaden op [http://www.viwta.be/files/Eindrapport_cyberpesten_\(nw\).pdf](http://www.viwta.be/files/Eindrapport_cyberpesten_(nw).pdf)

Hebben alle kinderen evenveel last van gepest worden?

Onze inschatting is dat niet alle kinderen op dezelfde manier reageren op gepest worden. Het is daarom voor opvoeders moeilijk om na te gaan welke invloed het pesten op een kind heeft. Bovendien schamen kinderen zich en trekken ze zich terug: ze laten dikwijls weinig merken van hun gevoelens als ze worden gepest. Het ene kind haalt zijn of haar schouders op, terwijl een ander kind niet meer naar school durft. Enkele adviezen voor het schoolbeleid zijn een duidelijk school- en sanctioneringsbeleid: "Een school met duidelijke en zichtbare regels voor het gebruik van computer- en communicatiemateriaal binnen de school, kan optreden als leerlingen en personeelsleden zich niet aan deze regels houden. Het corrigeren en sanctioneren van ongewenst gedrag in deze, is een taak van de schoolleiding" (Bron: www.ppsi.nl).

In de bovenstaande studie van het viWTA vind je nog tal van mogelijke acties om het pesten (in school) aan te pakken.

Kun je achterhalen wat er geschreven wordt tijdens een MSN-chat?

Ja, dat kan als je de optie 'Berichtengeschiedenis bijhouden' aanklikt. Hiervoor open je het MSN programma d.m.v. inloggen (hiervoor moet je dus wel de naam en het wachtwoord hebben) en kijkt bij opties. MSN verandert regelmatig van versie, dus het is even zoeken. Als de optie is aangeklikt, wordt een berichtengeschiedenis bijgehouden. Dit is trouwens ook een manier om in overleg met een kind na te gaan hoe het wordt gepest.

Het nieuwe chatprogramma Google Talk (wat op MSN lijkt) is nog te nieuw en te onbekend om er op deze plek nader op in te gaan. In elk geval vormt Google Talk (nog?) geen alternatief voor msn-en. Momenteel is Google Talk nog in testfase.

Zie ook: <http://weetwatjetypt.nl/>

Hoofdstuk 7 Lang, langer, langst!

Doel:

- Leerlingen kunnen omschrijven wat rsi is.
- Leerlingen kunnen de beste houding achter de computer omschrijven en kunnen deze kennis te gebruiken door van houding te veranderen.
- Leerlingen kunnen omschrijven wat ze moeten doen bij lichamelijke klachten.
- Leerlingen zijn zich bewust van de gevaren van computerverslaving.

Te behandelen onderwerpen:

- Wat is rsi?
- Hoe kun je het krijgen?
- Wat zijn de klachten en hoe herken je die? Wat moet je doen om het te voorkomen? Wat moet je doen als je klachten hebt?
- Hoe lang zit jij achter de computer?
- Hoe zit jij achter de computer/ Nintendo/ Playstation? Wat is een goede en wat is een foute houding?
- Wat is een verslaving?
- Waarom is verslaving niet goed?

Wat is ...

RSI = de bewegingsziekte rsi komt voort uit een verkeerde houding die te lang en te vaak is ingenomen, bijvoorbeeld door lang onderuitgezakt voor de computer te zitten.

Nintendo en Playstation = games, computerspelletjes

Gemiddelde tijdsinvestering: 1 lesuur

Evaluatie

Wat hebben we de vorige les gedaan en wat hebben we ervan geleerd? Bespreek nogmaals kort het verschil tussen gewoon pesten en het anonieme digitale pesten, wat je leerlingen hiertegen kunnen doen en hoe zij zich hiertegen kunnen wapenen.

Opdracht 18

- Titel: Lang, langer, langst!
- Leermiddelen: pennen
- Korte inhoud: Bespreek met de leerlingen in welke houding ze achter de pc zitten en hoe lang ze gemiddeld achter de pc zitten. Leg uit wat het woord ergonomie betekent en wat ergonomen zijn. Ergonomen houden zich o.a. bezig met het op een goede manier achter je computer zitten en hoe je je handen op het toetsenbord kunt plaatsen zonder dat je pijnlijke vingers en handen zult krijgen.
- De vraag die gesteld wordt is of de leerlingen wel eens lang achter een pc hebben gezeten. Waarom denken de leerlingen dat het niet goed is om zo lang achter een computer te zitten?
- Laat de leerlingen op de getoonde getekende pop met pijlen aangeven waar zij denken dat de meest kwetsbare plekken zitten.

Best laat je de leerlingen even de informatie lezen op de website www.rsi-vereniging.nl

→ Over RSI → Wat is RSI? (aandachtspunten bij lichamelijk onderzoek)

Antwoord: Te lang achter de computer zitten is niet goed voor je lichaam. Je kunt spierpijn krijgen in armen, schouders, nek of rug. Als je echt veel te lang en veel te vaak achter de computer zit, dan kan die spierpijn blijven en duurt het heel lang voordat het weer weg is. Pijlen in de tekening: polsen, armen, schouders, nek en rug.

Voor meer informatie over een goede werkhouding:

www.gezondheid.be/index.cfm?fuseaction=art&art_id=1315

www.rsi-vereniging.nl

Opdracht 19

Titel: Even kwissen
Leermiddelen: pen, eventueel computer
Korte inhoud: Bespreek nogmaals de houding die je aanneemt wanneer je achter een pc gaat zitten. Wat is een goede houding en welke houding is minder goed en waarom? Leg kort uit waar ergonomen mee bezig zijn. Wat weten de leerlingen zelf van rsi en hebben leerlingen zelf wel eens last gehad van pijnen wanneer ze te lang achter een computer hebben gezeten? Laat de leerlingen vertellen uit eigen ervaring. De leerlingen maken groepjes van twee tot vier leerlingen. Vervolgens mogen ze de vragen uit het oefenboek om ter snelst oplossen. Het groepje dat als eerste alle vragen juist heeft opgelost, is gewonnen. De leerkracht kijkt de oplossingen na; als er één of meer fouten zijn, moeten ze verder werken. De leerkracht kan ervoor kiezen om niet te zeggen welke vraag fout is beantwoord. Dit maakt het natuurlijk moeilijker. De leerlingen kunnen eventueel aan de computer het antwoord opzoeken. Ze kunnen daarbij een beroep doen op de websites:
www.microsoft.com/netherlands/hardware/ergonomie
www.ictopschool.net/infrastructuur/gezondcomputeren

Antwoorden 1 : c / 2 : b / 3 : c / 4 : a / 5 : a / 6 : a / 7 : a / 8 : a / 9 : a / 10 : b / 11 : b / 12 : a

Opdracht 20

Titel: Galgje (of een ander spel)
Leermiddelen: pc met internetverbinding
Korte inhoud: Leerlingen gaan op elkaars houding letten, terwijl ze een spelletje spelen op internet. Het spel Galgje kan je vinden op www.galgje.com. Je kan ook kiezen om een ander spel te spelen, zoals Patience; dit staat op elke Windows-computer. Eén of meerdere leerlingen zitten achter de pc en spelen het spel. Ze beginnen in de goede houding, zoals in het lesboek staat beschreven. Uiteraard zullen ze al snel van die houding afwijken als ze eenmaal aan het spelen zijn. Medeleerlingen mogen hen daarop aanspreken. Je kan er een spelelement aan toevoegen. De leerling begint met 10 punten. Elke keer dat een mede-leerling hem/haar moet corrigeren gaat er een punt af. Wie heeft na 10 minuten het hoogste aantal punten over?

Extra opdrachten

- Titel: Hoe lang?
Leermiddelen: pennen
Korte inhoud: Laat de leerlingen een week bijhouden hoeveel tijd ze besteed hebben achter de computer (een spelcomputer telt ook mee). Het maakt niet uit waar ze achter de computer hebben gezeten, thuis, op school of in het buurthuis. De leerlingen kunnen de tijden achter de dagen van de week plaatsen. Daarnaast tellen ze ook de tijden die ze buiten hebben gespeeld en verwerken die ook in het weekoverzicht. De leerlingen kunnen de twee overzichten met elkaar vergelijken en bij zichzelf nagaan of ze iets zouden kunnen veranderen aan hun tijdsbesteding. Bespreek kort de uitkomst van de overzichten met de gehele klas.
- Opmerking: Leerkrachten kunnen de leerlingen aanspreken op de houding die ze aannemen achter de computer op school. Leerlingen kunnen elkaar ook corrigeren op hun houding.

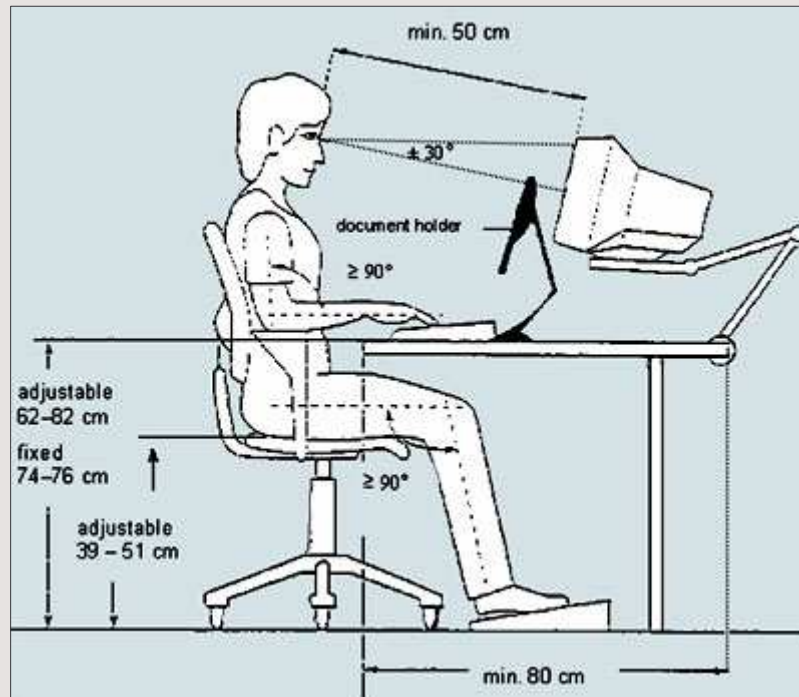
Meer informatie: www.ictopschool.net/infrastructuur/gezondcomputeren

- Titel: Goede houding
Leermiddelen: pennen
Korte inhoud: De leerlingen observeren de houding van de vrouw op de foto. Ze moeten vooral kijken naar de pols, schouders, nek, kijkafstand.
- Kijkafstand:* moet ongeveer 50 cm van je ogen staan; dus OK.
Toetsenbord: best zou die rusten op een polssteun. Tegenwoordig zijn er ook toetsenborden waar een polssteun aan vastzit, zoals hier.
Zithouding: zit recht.
- Geen informatie over de stoel, een voetensteun, het binnenklimaat, het scherm (schermflikkeringen, resolutie, enz.). Ook over de muis kan je weinig vertellen, vermits niet duidelijk genoeg.
- Het is vooral de bedoeling dat de leerlingen naar alle facetten kijken die de kans op RSI verminderen.

Achtergrondinformatie bij hoofdstuk 7

Rsi en verslaving

Rsi



Rsi is een verzamelnaam voor klachten, symptomen en syndromen die voorkomen in bovenrug, nek- en schoudergebied, armen, ellebogen, polsen, handen en vingers. De klachten worden doorgaans veroorzaakt door repeterende bewegingen, een langdurige statische houding of een combinatie van beide. Verder kunnen persoonsgebonden en werkgebonden factoren een belangrijke rol spelen bij het ontstaan, verergeren of het instandhouden van rsi. Rsi komt in veel beroepsgroepen voor.

Bron: www.rsi-vereniging.nl

Risico: RSI

Ook kinderen lopen de kans om rsi te krijgen. Rsi is een ziekte die op kan treden als men te lang in een bepaalde houding werkt. De lichaamshouding van kinderen is een zorg voor vele opvoeders. Ook jongeren hebben steeds meer last van rsi (zie artikel). Het aantal kinderen dat kampt met houdingsproblemen stijgt. In tegenstelling tot vroeger brengen veel jongeren hun tijd tegenwoordig zittend door, zowel thuis als op school. Dit heeft vooral te maken met een inactieve levensstijl. Bovendien hebben ze vaak een passieve en onderuitgezakte houding voor de televisie of achter de computer. Een onjuiste houding achter de computer kan leiden tot pijn in de nek, rug of bepaalde spieren, 'kinder-rsi'. Niet alleen de houding maar ook het materiaal en meubilair dat kinderen gebruiken zijn vaak niet op hun lichaam en lichaamslengte toegesneden. Er wordt inmiddels een aantal producten op de markt gebracht die speciaal voor kinderen zijn ontwikkeld, zoals een speciale kindermuis, geschikt voor de (kleinere) kinderhand. Ook bestaan er kleine laptopmuizen die beter geschikt zijn voor kinderhanden.

Test jezelf: www.gezondheid.be/INDEX.cfm?fuseaction=art&art_id=1368

Oplossingen

Kinder-rsi

In de lessen maken de kinderen kennis met een aantal (verkeerde en goede) lichaamshoudingen achter de computer. De adviezen voor de kinderen die worden gegeven zijn:

Bewegen achter de computer is goed. Achter de computer werken betekent vaak lang stilzitten in dezelfde houding. Dat is niet goed. Probeer toch zoveel mogelijk te bewegen achter de computer. Zo voorkom je dat je pijn krijgt in handen, armen, nek en rug.

Tips om te bewegen:

- Wisselen van houding, wisselen van bil, ga eens rechtop zitten, in elkaar zakken, iets naar achteren.
- Zwaai eens met je armen tussendoor of rek je eens uit.
- De muistoets is om iets aan te klikken en niet om steeds op te drukken. Dan krijg je pijn in je hand en kun je helemaal niet meer internetten.
- Draai eens met je nek als je achter de computer zit.
- Zit je al 15 minuten achter de computer? Dan wordt het tijd om eens wat te drinken te halen. Loop af en toe eens weg van de computer om iets anders te doen.
- Ga eens na hoe lang jij per keer achter de computer zit. Houd bijvoorbeeld met een kookwekker of met de stopwatch op je mobieltje de tijd bij.
- Weet je wanneer een monitor voor een kind op de goede hoogte staat? Daar kom je als volgt achter... Moet je naar boven kijken? Dan staat de monitor te hoog en krijg je last van je nek. Zet de stoel omhoog (bijv. thuis door een stoel die omhoog en omlaag kan) of ga op een kussen zitten. Moet je naar beneden kijken? Dan staat de monitor te laag. Dan krijg je last van je nek en rug. Zet de monitor hoger door een paar plankjes of oude boeken onder de monitor te leggen. De monitor staat goed wanneer je rechtop zit en net over het scherm heen kunt kijken.

Tips voor thuis:

- Zorg voor een stoel die je in hoogte kunt verstellen. Dus naar beneden of naar boven. Niet iedereen thuis is even groot, dus bij de één zal de stoel omlaag moeten, bij de ander juist omhoog. Zo kunnen jullie toch allemaal goed achter de monitor zitten.
- Zweven je voeten boven de grond? Zet dan een krukje of iets anders onder je voeten.

Risico: computerverslaving

Kinderen zijn vaak gek op computers. Sommige kinderen kunnen zodanig gefascineerd raken door chatten, mailen, surfen en downloaden, dat die fascinatie kan omslaan in verslaving. Bijvoorbeeld als ze een nieuw computerspel hebben gekregen waar ze helemaal 'verslingerd' aan raken. Na een tijdje kan het nieuwe aan zo'n spel (of een website of een chatbox) eraf raken, maar er zijn ook kinderen die gefascineerd blijven en verslaafd raken. Kinderen vervelen zich en daardoor grijpen ze naar computer (en/of tv). Ze volgen series (er zijn namelijk ook internet soapseries) en raken daardoor verslaafd. Ze spelen levels van computergames en die willen ze uitspelen. Ouders hebben weinig tijd om met hun kinderen bezig te zijn en kinderen gaan zoeken naar computergames en mogelijkheden om te chatten of te msn-en. Met alle gevolgen vandien. De kinderen maken hun huiswerk niet meer omwille van de computerverslaving. Ze stellen altijd hun dagelijkse werken (de vaat, de tafel afruimen) uit. Door de verslavende programma's of verslavende spelletjes doen de kinderen niet meer aan sport.

De kinderen komen daardoor niet buiten. Door de programma's worden de kinderen gewelddadig of zenuwachtig. De kinderen kunnen problemen hebben aan de ogen door te dicht op de monitor te zitten. Gecombineerd met de verslaving kan kinder-rsi optreden.

Oplossingen

Eigenlijk valt computerverslaving in hetzelfde rijtje als andere verslavingen. Hier volgen enkele adviezen om kinderen van hun computerverslaving af te helpen:

- Hoe lang zit je al achter de computer? Neem eens de tijd op! Bewegingsexperts vinden 40 minuten per dag het maximum om achter de computer te zitten: hoeveel minuten zit jij er meer achter?
- Denk je dat je buiten de computer kunt? Waarom wel/niet?
- Denk je dat je computerverslaafd bent geraakt? Waarom denk je dat?
- Probeer eens wat anders te doen. Zet bijvoorbeeld een kookwekker om te klokken hoe lang je al bezig bent.
- Heb je andere hobby's buiten computeren? Ga die doen.

Vragen en antwoorden

Ik merk als leerkracht dat één van mijn leerlingen te vaak en te veel achter de computer zit. Zijn huiswerk lijdt er duidelijk onder. Hij komt doodmoe op school. Wat kan een school hieraan doen?

Je zou kunnen praten met de ouders en proberen erachter te komen of je vermoeden klopt. Het zou het beste zijn als je samen met de ouders op dezelfde lijn kwam. Zo kan je samen het probleem van deze vermoeide leerling aanpakken. Het is ook van belang dat de leerling er zelf achter komt dat zijn/haar mate van computeren problemen geeft. Echter, thuis zullen oplossingen bedacht moeten worden.

Op school hebben we geen computermeubilair en -apparatuur die speciaal voor kinderen is gemaakt. Is dat erg?

Op veel scholen kunnen kinderen geen gebruik maken van speciaal meubilair en apparatuur als het om computers gaat. Als er geen budget is om tot aanschaf over te gaan, kan je wel de adviezen opvolgen die deskundigen geven om meer op je leerlingen gerichte mogelijkheden aan te bieden. Bijvoorbeeld: de hoogte van de monitoren en de afgestelde stoelen, gebruik maken van een voetenbankje of kussen om op te zitten.

Hoofdstuk 8 Internet is cool

Doel:

- Leerlingen zijn zich bewust van eigen handelen op internet.
- Leerlingen kunnen zich online gedragen.
- Leerlingen spreken anderen aan op hun internetgedrag.
- Leerlingen bespreken het internetprotocol met hun ouders.
- Leerlingen stellen voor thuis een protocol op.

Te behandelen onderwerpen:

- Hoe gedraag je je op internet?
- Hoe doe je je voor op internet?
- Wat doe je wel en wat doe je niet?
- Maak internetregels voor de klas.
- Maak internetregels voor thuis.

Gemiddelde tijdsinvestering: 1 lesuur

Evaluatie

Wat hebben we de vorige les gedaan en wat hebben we ervan geleerd? Bespreek nogmaals hoe belangrijk het is om een goede houding te hebben wanneer je achter de computer zit.

Opdracht 21

Titel: Internet is cool
Leermiddelen: vel papier, pennen
Korte inhoud: Bespreek samen met de leerlingen hoe je je zou kunnen gedragen op internet. Maak een vergelijking met het verkeer. 'Het verkeer kent ook regels. Die regels moet je leren om veilig aan het verkeer te kunnen deelnemen. Je krijgt zelfs les op school met daarop volgend een verkeerseexamen.'

In de voorgaande lessen hebben de leerlingen kennis kunnen nemen van hoe je je gedraagt op internet en wat ze kunnen doen wanneer ze ongewenste en onverwachte dingen tegenkomen. Je legt aan de leerlingen uit wat er met het woord netiquette bedoeld wordt. De ongeschreven regels op internet waar je je aan moet houden.

De opdracht is dat de leerlingen in groepen van twee of vier verdeeld worden. Iedere groep krijgt een vel papier. Dit vel verdelen ze in vier vakken, met in het midden een groter vak. Iedere leerling van de groep schrijft een regel op het papier die hij of zij belangrijk vindt naar aanleiding van de volgende stellingen:

- Wat vind je dat wel mag op school?
- Wat vind je dat niet mag op school?
- Aan welke regels moet een leerling zich houden?
- Als iemand zich niet aan de regels houdt, wat is dan de straf?

Wanneer iedere leerling van een groep de regels heeft aangeleverd bespreekt de groep met elkaar wat zij de belangrijkste regels vinden. Ze schrijven die in het middenvak van het papier. De belangrijkste regel zetten ze bovenaan in het vak. Daarna kan je klassikaal bespreken welke regels de groepen hebben bedacht en opgeschreven.

Klassikaal maken de leerlingen nu een internetprotocol voor de gehele

school.

Wat is ...

Netiquette = een samentrekking van de woorden Net (een ander woord voor internet) en Etiquette. Netiquette houdt in: de gedrags-normen hoe er met elkaar wordt omgegaan op internet.

Opdracht 22

Titel: Wat doen zij?
Leermiddelen: pennen
Korte inhoud: De leerlingen herkennen het onveilige gedrag van de personages en denken zelf na over een goede oplossing. Jonas geeft zijn e-mailadres. Tine geeft min of meer haar wachtwoord.
Laura krijgt spam. Muzaffer klikt op een betaald spelletje en krijgt nepberichten binnen.

Antwoorden: *Muzaffer: bellen om een spelletje online te kunnen spelen en het ontvangen van vreemde e-mail, die hij gelukkig wel weggooit. Tine: klikken op banners die vertellen dat je geld kunt verdienen en het hebben van een veel te makkelijk wachtwoord. Jonas: komt 'rotzooi' tegen op internet die hij wegklikt.*

Extra opdrachten

Titel: Als ik de baas van internet was
Leermiddelen: pennen, papier
Korte inhoud: De leerling gaat een opstel schrijven met als titel 'Als ik de baas van internet was'. Dit opstel kan gebruikt worden voor bijvoorbeeld de nieuwsbrief of de website van de school.

Titel: Internet-speurtocht
Korte inhoud: Door het maken van een speurtocht wordt de zoekvaardigheid van de leerlingen op het internet vergroot. De bedoeling is dat ze steeds beter en gericht weten te zoeken op het internet. Gebruik de gemaakte speurtochten niet alleen in de klas. Je kan ze ook plaatsen in de nieuwsbrief, de schoolkrant of op de schoolwebsite. Dit kan andere leerlingen en/of ouders stimuleren om samen actief bezig te zijn op het internet.
Leermiddelen: pennen en een pc met internetverbinding

Onderstaande opdrachten staan niet vermeld in het werkschrift van de leerlingen.

Titel:	Ganzenbord
Leermiddelen:	Stevig kartonnen vel, stevig papieren vel, potlood/stiften, schaar, lijm, dobbelsteen, pionnen
Korte inhoud:	Je kent vast en zeker het welbekende ganzenbordspel. Met een dobbelsteen wordt geworpen, en per pion wordt er over het bord 'gelopen'. Tijdens het ganzenbordspel kan de pion in de put raken, en zelfs helemaal opnieuw moeten beginnen. Je leerlingen gaan nu een variatie op het spel maken, die natuurlijk alles te maken heeft met internet. Smileys staan hierbij centraal. Door een ganzenbordspel te maken en te spelen blijven de leerlingen actief bezig met het onderwerp en blijven de termen en materie door middel van herhaling beter 'hangen'.

Internet Ganzenbord

Maak een eigen ganzenbordspel.

Hoe maak je een ganzenbordspel?

Je maakt groepen van twee, drie of vier kinderen.

Een ganzenbord bestaat altijd uit vakjes met een nummer. Teken minimaal 40 hokjes.

Bedenk acht gebeurtenissen die te maken hebben met veilig internetten om in het spel te verwerken.

Bedenk voor elke gebeurtenis een figuurtje om op het spelbord te tekenen.

Bijvoorbeeld een hele blije smiley. Gebeurtenis: Je bent een kanjer. Je hebt geen privé-gegevens doorgegeven op internet. 2 plaatsen vooruit. Of een boze smiley. Gebeurtenis: Je hebt een virus op de computer. 6 plaatsen terug.

Tips voor de leerlingen:

Je kunt ook de plaatjes van Muzaffer, Tine, Jonas en Laura kopiëren, uitknippen en op het spelbord plakken.

Schrijf de gebeurtenissen op een apart vel. Schrijf daarachter hoeveel plaatsen iemand vooruit of achteruit moet.

Voorbeeld

Nummer	Gebeurtenis	Hoeveel plaatsen
Hokje 3	Kanjer. Je hebt geen privé-gegevens doorgegeven op internet.	2 plaatsen vooruit
Hokje 9	Je hebt een virus op de computer.	6 plaatsen terug

Titel:	Tentoonstelling
Leermiddelen:	scharen, lijm, karton, printerpapier, tijdschriften, stiften/potloden
Korte inhoud:	Je leerlingen hebben de afgelopen lessen veel geleerd over veilig internetten. Natuurlijk is hierover ook een tentoonstelling te maken! Bijvoorbeeld om de ouders te laten zien wat de kinderen geleerd hebben. En misschien kunnen de ouders weer van de ervaringen van de leerlingen leren? Ook voor de leerlingen is het goed om met het maken van deze tentoonstelling alles nogmaals te herhalen en door te nemen.

Hoe kan deze tentoonstelling eruit zien?

- Collage over veilig internetten, bijvoorbeeld:
 - Een collage over de top 5 van leukste kinderwebsites
 - Een collage over de top 5 van vervelende dingen op internet
 - Een collage over pop-ups
 - Een collage over reclames
 - Een collage over spelletjes op internet
- De interviews die gehouden zijn
- De ganzenbord spellen
- Natuurlijk een paar computers met internet, dan kunnen de ouders direct hun kennis testen
- De internet gedragsregels die in groepjes zijn gemaakt

De leerlingen kunnen vast nog meer bedenken om in de tentoonstelling te verwerken.

Achtergrondinformatie bij hoofdstuk 8

Internet gedragsregels

Wat zijn internet gedragsregels?

Je leerlingen leren om te gaan met de risico's van internet. Je school ziet het belang hiervan in; daarom bied je je leerlingen deze cursus aan. Daarnaast raden we je aan om voor de school bij aanvang van elk schooljaar een **internetprotocol** op te stellen tussen directeur, leerling en ouders. Dit protocol is erop gericht om ook op school met internet voor de leerlingen een zo veilig mogelijke omgeving te bieden. In het internetprotocol staan de gedragsregels, waar de leerlingen zich met betrekking tot internetgebruik op school aan moeten houden.

Er zijn al veel scholen die een dergelijk protocol hebben. Natuurlijk heeft het opstellen van een dergelijk protocol alles te maken met de identiteit van je school. Je onderwijsideeën en -gedachtegoed hebben hun weerslag in wat je waardevol vindt in het door de leerlingen omgaan met internet. In de lessen wordt de leerlingen de kans geboden om mee te denken wat voor soort regels er gesteld kunnen worden. Deze keuze is gemaakt omdat ook kinderen horen na te denken wat bijvoorbeeld de verschillen zijn tussen internet op school en internet thuis, en welke manieren er gevonden moeten worden om problemen met internet te voorkomen.

Welke regels kunnen er met betrekking tot surfen gesteld worden? Sommige scholen hebben met hun leerlingen afgesproken dat als het voorkomt dat een leerling (onbedoeld) op een verkeerde site terecht komt, het kind dit vertelt aan de juf of meester. Voor een kind dat bewust (en dus ernaar zoekend) op zulke sites komt, wacht de straf dat hij/zij voorlopig niet achter de pc mag. Vaak wordt er een internetprotocol door scholen opgesteld omdat er in het verleden iets is misgegaan. In het lesmateriaal wordt aandacht besteed aan het opstellen van internetregels voor de school. Je kan ook (alvast) bekijken wat collega-scholen hebben opgesteld.

Voorbeeld van een protocol

(Bron: www.ond.vlaanderen.be/ict/ondersteuning/veiligICT/)

Hierna vind je een voorbeeld van een protocol. Regels kunnen naar believen aangepast of aangevuld worden. Het ICT-protocol kan ook deel uit maken van het schoolreglement. Dit protocol zal vanzelfsprekend bruikbaar zijn in het secundair onderwijs dan in het lager onderwijs.

Internetprotocol Internetprotocolpag. 1

Onze school beschikt over een uitgebreid computerpark dat door een grote verscheidenheid aan gebruikers dagelijks intensief gebruikt wordt. Het onderhoud van een dergelijk park is meer dan een fulltime job. Dagelijks zijn de informaticacoördinatoren, maar ook héél wat leerkrachten informatica in de weer om het netwerk in prima conditie te houden. Dankzij de inzet van die vele mensen kan elke leerling elke informatica- en/of dactyloles beschikken over een goed werkend toestel. Maar ook buiten de lessen krijgen de leerlingen de kans om van de computer infrastructuur gebruik te maken, denken we maar aan de computerstudie en het cybercafé.

Om deze zaken te kunnen blijven garanderen, eisen wij van onze leerlingen dat ze de computer infrastructuur professioneel gebruiken. Concreet hebben we een aantal aandachtspunten opgesteld waaraan elke leerling zich dient te houden:

Toegang tot het computerlokaal

1. Het computerlokaal is alleen toegankelijk op volgende dagen en uren:
Maandag: van ... tot ... en van ... tot ...
Dinsdag
...
2. Leerlingen worden enkel toegelaten onder begeleiding van een leerkracht, indien op voorhand gereserveerd werd.
3. Individuele leerlingen kunnen aan de beheerder/ICT-coördinator toelating vragen om in het computerlokaal te werken. Zij moeten daartoe een specifieke opdracht kunnen voorleggen.

Gebruik van de computers

1. Bij het werken aan een computer vult de leerling eerst het logboek van die pc in.
2. Het is niet toegelaten nieuwe software op de pc's te plaatsen of de instellingen te wijzigen. Met het oog op het vermijden van virussen mogen geen eigen diskettes of CD-ROMS worden gebruikt, enkel schooldiskettes.
3. Het is niet toegelaten de hardware (PC's, printers) af te koppelen of te verplaatsen.
4. Indien er problemen zijn met een computer of het netwerk, dan is het de taak van de leerling om de leerkracht hiervan op de hoogte te brengen. Probeer het probleem niet zelf op te lossen.
5. Afdrukken maken kan enkel tegen betaling. Bestanden kunnen meegenomen worden op een schooldiskette.
 - het tarief voor afdrukken bedraagt {bedrag} euro per afdruk
 - de kostprijs van een schooldiskette bedraagt {bedrag} euro per diskette
6. Indien een leerling opzettelijk schade berokkent, zal hij/zij deze moeten vergoeden. Onder opzettelijke schade wordt hier o.a. verstaan:
 - het wijzigen van en/of schade toebrengen (graffiti inbegrepen) aan de hardware;
 - het besmetten van het systeem met virussen;
 - het wissen of wijzigen van instellingen en van de software die ter beschikking staat van de leerlingen;

- ...

Internetprotocol pag. 2

Gebruik van internet

1. Het gebruik van internet kan alleen op volgende dagen en uren:
Maandag: van ... tot ... en van ... tot ...
Dinsdag
...
2. Het gebruik van internet is gratis maar kan enkel indien het bedoeld is voor het vervullen van schoolopdrachten. Hetzelfde geldt voor chatten en het gebruik van nieuwsgroepen en e-mail. Ook dit kan enkel in het kader van schoolopdrachten.
3. Het bekijken van porno, racistische of andere discriminerende websites is verboden.
4. Elke toepassing die de leerling realiseert – voor zichzelf of ten opzichte van derden – in verband met school of met kennis die via de school kan verworven zijn, is vrij van pornografische, racistische, gewelddadige of mensonterende inhoud; ze beantwoordt aan alle elementen van de wet op de privacy en van de wet op het auteursrecht; ze bevat geen informatie die kan beledigen, kwetsen of schade berokkenen.
5. Op het internet respecteer je de 'netiquette'. Op welke wijze je ook met andere mensen in contact komt (vb. e-mail/chat) je blijft ten allen tijde beleefd.
6. Het downloaden van grote bestanden (> 500 KB) is enkel toegelaten na toestemming van een leerkracht.

We zijn er ons van bewust dat onze leerlingen zich nog in een leerproces bevinden. We willen duidelijk stellen dat we pas zullen sanctioneren als de afspraken doelbewust worden overtreden.

Voor akkoord,

{handtekening}

{handtekening}

{handtekening}

De directeur

De leerling

De ouders

{Datum}

Voorbeeld 2 van een Internetprotocol

Stedelijke Basisschool Kermt - Spalbeek ICT in onze school

algemeen

historiek

in onze school

eindtermen

surf safe ...

Surf safe:



Op school wordt er gewerkt op het internet onder begeleiding. Maar dat kan elders niet steeds, vandaar deze 7 basisregels om kinderen veilig te leren surfen.

1. Ik leg uit aan mijn ouders wat ik doe op het internet.
2. Ik geef nooit zomaar mijn naam, adres, telefoonnummer of foto aan iemand die ik heb leren kennen via het internet, zelfs als die erom vraagt.
3. Mijn paswoord is strikt persoonlijk, ik verklap het aan niemand. Het is een beetje als de sleutels van mijn huis: ik geef ze niet aan gelijk wie.
4. Als ik iemand met wie ik via het internet kennism gemaakt heb in het echt wil ontmoeten, overleg ik eerst met mijn ouders.
5. Ik beëindig elke communicatie en ik verwittig mijn ouders zodra ik informatie ontvang, deelneem aan gesprekken of beelden tegenkom, waarbij ik me ongemakkelijk voel.
6. Ik geloof niet alles wat ik zie en hoor op het internet. Ik leer kritisch te zijn.
7. Wanneer ik via het internet communiceer, blijf ik altijd fatsoenlijk. Ik doe niets dat andere personen kan kwetsen of ongemakkelijk maakt.

Als je toch informatie of beelden ontvangt die als storend of schokkend ervaren worden, stuur ze dan door naar:

surfsafe@childfocus.org

Meer info: www.childfocus.org

Richtlijn

Natuurlijk biedt een protocol niet de garantie dat op school tijdens het internetgebruik nooit meer iets vervelends gebeurt. Maar een protocol kan wel als richtlijn gelden. Een serie afspraken, waar de school op terug kan vallen mocht er inderdaad iets mis (zijn ge)gaan. Bovendien weten leerlingen, leerkrachten, en ook ouders door het bestaan van een dergelijk protocol welke regels en sancties op school gelden.

Netiquette

Al in 1995 stelde de internetgemeenschap een reeks informele regels op om het internet leefbaar te helpen houden. Deze "netiquette" blijkt nog steeds verrassend actueel. Voor jeugdige en/of beginnende gebruikers van chat en e-mail is een initiatie in de regels van de netiquette de eerste stap naar een efficiënte en stijlvolle elektronische communicatie.

Netiquette is een gedragscode die bedoeld is om de communicatie op het internet efficiënt en fatsoenlijk te houden. Ze is erg uitgebreid want er zijn verschillende communicatiekanalen (e-mail, chat, nieuwsgroepen en mailinglijsten) en het is geen eenvoudige zaak om de ongeschreven regels daarvan te kennen.

Er bestaan enerzijds ethisch getinte voorschriften over de veiligheid van de gebruikers, het berichtformaat, de belasting van het netwerk en de server. Anderzijds komt bij netiquette ook veel taalkunde kijken. Zoals bekend laten beginnende internetgebruikers zich snel verleiden tot onverzorgd of onbeschoft taalgebruik. Dat ligt aan de aard van het medium: de communicatie bij e-mail, chat en nieuwsgroepen verloopt meestal informeel en per definitie flitsend. Het is trouwens een vaak gehoorde verzuchting onder leraren taalkunde dat jongeren vervallen in fonetisch gebrabbel wanneer ze zich in een virtuele ruimte bewegen.



Enkele voorbeelden van ethische netiquette:

- doe niet mee aan kettingbrieven of rampberichten
- neem enige reserves in acht bij het doorsturen van e-mails
- maak een onderscheid tussen beantwoorden en allen beantwoorden
- Enkele voorbeelden van taalkundige netiquette
 - Korte teksten Schrijf korte en bondige teksten, zonder in een telegramstijl te vervallen die aanleiding kan geven tot misverstanden.
 - Onderwerp Geef een bericht een duidelijk onderwerp mee. Zo dringt de essentie van de e-mail door.
 - Toon: het informele karakter en de afstand tot de geadresseerde zorgt ervoor dat men zich wat makkelijker uit in een e-mail bericht. Dat kan echter negatief werken als men ontstemd is over iets; het resultaat is dat de teksten dan vaak feller zijn dan men gewoon is. Lees een dergelijk bericht daarom opnieuw door en overweeg of je een dergelijke tekst ook rechtstreeks tegenover de geadresseerde zou uitspreken.
 - Humor: wees voorzichtig met grappen en sarcasme, gebruik liever emoticons zoals :-) het lachebekje en ;-)- de knipoog.
 - Hoofdletters: gebruik geen hoofdletters waar het niet hoeft. Ze zijn schreeuwerig en onbeleefd.

6 Interessante websites

Eindtermen

www.ond.vlaanderen.be/dvo/basisonderwijs

Algemene sites over veilig internetten

www.childfocus.org (meldpunt)

www.clicksafe.be (veilig surfen)

www.saferinternet.be → Pers (berichtgeving over internet en jongeren)

www.klasse.be/archief/index.php?op=archief&nr=9408 (wat weet je over veilig internet?)

www.digibewust.nl (overheids campagne)

veilig.kennisnet.nl (info en tips voor alle gebruikers in het onderwijs)

www.technika10.nl/internetoke (Technika 10 Nederland)

www.kinderconsument.nl (voor ouders, leerkrachten en kinderen)

www.msn.nl/veiligonline (voor ouders, leerkrachten en kinderen)

www.surfsafe.nl (voor kinderen, tieners en opvoeders)

www.mijnleerlingonline.nl (Planet Internet i.s.m. Ouders Online)

www.mijnkindonline.nl (idem)

www.europa.eu.int/ISPO/iap (safe use of internet Action Plan)

www.diplomaveiliginternet.nl

Kinderen en chatten

‘veilige chatboxen’

<http://www.chat.be>

<http://www.skynet.be> via www.kidcity.be

<http://breedband.telenet.be>

<http://www.krey.net/saferchat/>

Algemene informatie

www.clicksafe.be

<http://to.be/content/veilig.php>

www.saferchat.be

www.digikids.be

<http://users.skynet.be/karendm/> een kwisje over veilig chatten

www.chatinfo.nl (initiatief van chatboxhouders in Nederland)

www.internetsoa.nl (voorlichting aan kinderen en pubers over sex en internet)

Filterprogramma's

www.veiligophetnet.nl

www.ictopschool.net (onderzoek filters)

www.ictopschool.net/infrastructuur/publicaties/uitgaven/filter/index.html

<http://onderwijs.vlaanderen.be/publicaties/eDocs/pdf/145.pdf>

Kinderbrowsers

Look4 www.look4.be
Scaldia www.scaldia-soft.nl/kindvriendelijk.htm
Kidnet Explorer www.resource-communications.com/kidnet.html
Tiscali Kids <http://www.tiscali.nl/diensten/kids/default.asp>
Krowser www.krowser.nl
Chibrow www.chibrow.com
Meestersipke www.meestersipke.nl
Netwijs www.netwijs.nl
Watikzoek www.watikzoek.nl
Samenzoeken www.samenzoeken.nl

Meldpunten

www.childfocus.org
www.nedbel.be/internetpolitie.htm
<http://www.ecops.be/> (een online meldpunt van de politie)
www.limits.be (vzw over pesten op school)

Studiedagen rond veilig internet

www.actioninnocense.org
www.degezindsbond.be
www.nedbel.be

Digitaal pesten

www.cyberpesten.be
[http://www.viwtat.be/files/Eindrapport_cyberpesten_\(nw\).pdf](http://www.viwtat.be/files/Eindrapport_cyberpesten_(nw).pdf)
www.msn.be/security/inbox/
<http://ludit.kuleuven.be/software/beveiliging/mailclient.html>
www.edublogs.be/2007/01/18/cyberpesten
www.saferinternet.be
www.klasse.be/kvo/94/6
www.life1215.be/html/ikendeander/vrienden/cyberpesten
www.stopdigitaalpesten.nl (SIRE campagne)
www.pesten.net (zelfhulp site van en voor kinderen)
www.sjn.nl/pesten (informatie over pesten en oplossingen)
www.pestenislaf.nl
www.vios-amsterdam.nl (project tegen Cyberpesten)
www.ppsi.nl (hulp via het Platform Preventie Seksuele Intimidatie)
<http://weetwatjetypt.nl/>

Over rsi bij kinderen

www.rsi.be
www.gezondheid.be/index.cfm?fuseaction=art&art_id=1315
www.gezondheid.be/INDEX.cfm?fuseaction=art&art_id=1368 (test jezelf)
www.rsi-vereniging.nl (rsi patiëntenvereniging)
rsi.startpagina.nl (overzicht van allerlei websites over rsi)

Over computerverslaving bij kinderen

<http://www.ond.vlaanderen.be/schooldirect/BL303/ICT4.htm> (geen pc voor 14?)
www.ouders.nl (forum voor ouders, ook over internetende kinderen)

Onderzoek over kinderen en internet

www.uvv.be/uvv5/pub/cinfo/jo/pdf/01.pdf
www.insites.be/file.asp?filetype=doc/04/press_releases/20030424_NL_YOL.pdf
www.hetjongerenonderzoek.nl van P. Sikkema (2005)
www.hetjongerenonderzoek.nl
www.ivo.n

School en internet

www.ond.vlaanderen.be/ict/ondersteuning/veiligICT/ (voorbeeld protocol)
veilig.kennisnet.nl (informatie over veilig internet)
www.ictopschool.net (onderzoek over filtering)
www.computersopschool.nl (blad over computers op school)
www.vives.nl (blad over computers op school)
(APS) www.computersindeklas.nl (webmagazine)

Virussen, spyware, spam, pop-up, ...

antivirus.startpagina.be
www.bipt.be/virus
www.robinsonlist.be
www.microsoft.com/belux/nl/athome/security/default.aspx
www.adcom.be
<http://www.lavasoftusa.com/software/adaware/> (anti spyware software)
<http://www.safer-networking.org/> (spybot)
ictopschool.startpagina.be/
ludit.kuleuven.be/software/virus.html
www.belgium.be/peeceefobie/
<http://beveilig.uwpc.info/>
www.telenet.be/nl/thuis/internet/veiligheid/anti-virus/index.page (met videofragment)
<http://ludit.kuleuven.be/software/beveiliging/popup.html>
<http://ludit.kuleuven.be/software/beveiliging/spyware.html>
<http://www.nedbel.be/anti-spyware.htm>
www.surfnet.nl
www.mcafee.com
www.symantec.com
mineco.fgov.be/protection_consumer/fraud_prevention/folders/Telephone_nl.pdf
(consumentenbescherming – spam)

Kids ID

<http://www2.dnsmaster.be>, www.saferchat.be,
<http://eid.belgium.be/nl/navigation/documents/42993.html>
www.eidsite.be/node/32

7 Interessante literatuur

Veilig internet

Mag ik op de computer? Computers en het internet in de opvoeding.

Auteurs: M. Valcke

Uitgave: Lannoo

Computers en internet, thuis en op school. Een inventariserend onderzoek bij lagere schoolkinderen.

Auteurs: M. Valcke en L. Oosterlinck

Uitgave: Gent: Universiteit Gent

Test-Aankoop. Wat glipt er door de mazen van het net? Test van 18 internetfilters. Nr. 452, maart 2002, pp. 18 e.v.

Clickx. Kinderen niet toegelaten. Censuursoftware. Clickx nr. 12, april 2002, pp. 56 e.v.

Insites E-research & consulting, Youth online 5.0, 2007 (www.insites.be)

Mijn Kind Online

Auteurs: Justine Pardoën, Remco Pijpers

Uitgave: SWP

SBN: 90 666 55 77

Mijn leerling Online:

Auteurs: Justine Pardoën, Remco Pijpers

Uitgave: SWP

SBN: 9066657324

Verliefd op Internet

Auteurs: Justine Pardoën, Remco Pijpers

Uitgave: SWP

SBN: 9066657847

Pandora's Mailbox, gids voor een kindveilig internet

Auteur: Bamber Delver, stichting De Kinderconsument

Uitgave: Easy Computing, 2003

SBN: 90 456 3465

Vet Veilig Internet

Auteur: Bamber Delver

Uitgave: Vives Media

SBN: 90809076-3-4

Computeren, leuk en leerzaam (een praktische gids voor ouders)

Auteur: Jolein de Rooij

Uitgave: Computer Idee/VNU Business Publications, 2003

SBN: 90 5855 146 6

Slim en Safe Internetten, veilig internet voor en door kinderen

Auteur: Bamber Delver

Uitgave: Kinderconsument i.s.m. Vives Media

SBN: 9080907618

Technika10.NL, internet oké voor kinderen

Internetcursus voor jonge kinderen

Auteur: S. de Ruiten, Technika 10 Nederland

Uitgave: Technika 10 Nederland

8 Moeilijke woordenlijst

A

ADSL	Supersnelle internetverbinding
Anti-virus software	Een programma dat virussen van je computer af kan halen.

B

Banner	Een reclameblokje op internet. Meestal zijn het bewegende plaatjes.
Blokkeren	Iets of iemand de toegang ontzeggen.
Browser	Een programma waarmee je op internet kunt surfen.
Bijlage	Via e-mail kun je bestanden meesturen met een bericht. Het bestand zit in de bijlage. Een bijlage herken je doordat er rechtsbovenin een paperclip staat.

C

Cammen	Via een webcam videobeelden naar een ander sturen.
Chatbox	Een webpagina op internet waar je kunt kletsen met anderen. Vaak zijn dit mensen die je niet kent.
Chatten	Kletsen via internet of via een messenger.
Cheats	Hulpjes om in een spelletje zonder veel moeite tot een hogere score te kunnen komen.

D

Dialer	Een programma dat geïnstalleerd wordt op je computer, waarmee je inbelt op een duur telefoonnummer.
Digitaal pesten	Pesten via internet, zoals via e-mail, chat of messenger.
Diskette	Een zwart vierkant schijfje waar je teksten en andere informatie op kunt zetten.
Downloaden	Bestanden van internet op je eigen computer zetten.

E

E-mai	Engels: Electronic mail. Een brief via internet versturen.
Ergonomisch	Een goede houding

F

Firewal	Een vuurmuur. Een bescherming voor je computer om te voorkomen dat vreemden in je computer kunnen inbreken.
---------	---

H

Hoax	Een nepbericht dat verstuurd wordt via e-mail.
Hyperlink	Een verwijzing naar een andere webpagina. Als je met de muis op een link gaat staan verandert het pijltje in een handje. Dan kun je klikken.

M

Messenger	Een programma waarmee je met anderen kunt kletsen. Je kunt alleen kletsen met mensen die je in je adreslijst van de messenger hebt staan. Een hele bekende is bijvoorbeeld: MSN.
-----------	--

N

Nettiquette	Ongeschreven regels over hoe je je moet gedragen op internet.
Nickname	Een bijnaam op internet

P

Privé-gegevens	Informatie over jezelf, die je niet meteen aan een ander vertelt.
Pop-up	Een klein venster dat vanzelf opent als je naar een website surft. Meestal staat er reclame in de pop-up.
Pop-up killer	Een programma dat de pop-up vensters blokkeert.
Profielen website	Een website waar je een eigen pagina kunt maken waar je iets over jezelf vertelt.

S

Spam	Ongewenste e-mail of e-mail waar je je nooit voor aangemeld hebt. Meestal zijn het e-mails met reclame erin.
Spamfilter	Een programma dat je op je computer moet installeren. Dit programma houdt spam tegen of zet de spam direct bij de Verwijderde Items in je e-mail programma.
Spyware	Een klein bestandje dat ongemerkt op je computer wordt gezet. Hiermee kunnen anderen bijhouden wat je doet op internet.

U

Updates	Nieuwe gegevens van een programma, die je meestal via internet moet downloaden. Bijvoorbeeld updates voor de virusscanner. Dan is je computer beschermd tegen de nieuwste virussen.
---------	---

V

Virus	Een programma dat je computer kan besmetten en ervoor kan zorgen dat je computer kapot gaat.
Virusscanner	Een programma dat virussen van de computer kan halen.

W

Webcam	Een kleine camera die je op de monitor van je computer kunt zetten. Als je de camera aanzet kun je de videobeelden of foto's naar een ander aten sturen.
Webpagina	Eén pagina op internet. Net zoals één bladzijde uit een boek.
Websserver	Een grote computer waar heel veel websites op staan. Net zoals een bibliotheek waar heel veel boekenkasten staan.
Website	Eén boek op internet. Net zoals één boek in een boekenkast.
Webmai	E-mailen via een programma op internet. Bijvoorbeeld met hotmail.

Z

Zoekmachine	Een pagina op internet, waar je websites kunt opzoeken door een zoekwoord in te typen en het programma te laten zoeken.
Zoekwoord	Een woord dat je intypt in een zoekmachine. De zoekmachine gaat zoeken naar webpagina's waar dat woord in voor komt.

Colofon

www.ond.vlaanderen.be/dvo/basisonderwijs/lager/uitgangspunten/ict.htm “Lager onderwijs - uitgangspunten ICT”.

www.ond.vlaanderen.be/dvo/basisonderwijs/lager/eindtermen/ict/htm “lager onderwijs - leergebiedoverschrijdende eindtermen ICT”.

www.ond.vlaanderen.be/ict/beleid/ETfaq FAQ eindtermen ICT

[http://ond.vsko.be/pls/portal/docs/PAGE/VVKBAORUBRIEKEN2006/PEDAGOGISCH EONDERSTEUNING/ICT/ICT%20DOELEN%20EN%20ET%20\(2\).PDF](http://ond.vsko.be/pls/portal/docs/PAGE/VVKBAORUBRIEKEN2006/PEDAGOGISCH_EONDERSTEUNING/ICT/ICT%20DOELEN%20EN%20ET%20(2).PDF) “aan ICT-doelen werken in het basisonderwijs”

Stichting Technika 10 Nederland



Stichting De Kinderconsument



Stichting Kennisnet / Ict op School



Ministerie van Economische Zaken



Ministerie van Onderwijs, Cultuur en Wetenschap



Vormgeving Ministerie van Economische Zaken, afdeling PGF

Auteur lesboek: S. de Ruiter, Stichting Technika 10 Nederland

Vlaamse versie: Michel Janssens, Xios hogeschool Hasselt

Auteur werkschrift: S. de Ruiter, Stichting Technika 10 Nederland

Vlaamse versie: Michel Janssens, Xios hogeschool Hasselt

Auteurs docentenhandleiding: B. Delver, M. Holtslag en L. Otten, Stichting de

Vlaamse versie: Michel Janssens, Xios hogeschool Hasselt

Kinderconsument, S. de Ruiter, Stichting Technika 10 Nederland

Eindredactie: B. Bloem, Stichting Technika 10 Nederland

De auteurs van het lesmateriaal hebben hun uiterste best gedaan om websites in dit lesmateriaal te vermelden die gedurende lange tijd beschikbaar zijn. Het team is niet verantwoordelijk en aansprakelijk voor externe websites die niet langer bestaan, evenals voor de inhoud van deze websites hoewel deze voor publicatie van dit boek zorgvuldig gescreend zijn.