VEILIG ONLINE

TIPS VOOR VEILIG ICT-GEBRUIK OP SCHOOL

Vlaamse overheid

Voorwoord

Wie afgaat op de alarmberichten in de media, begint misschien wel te denken dat ICT een doos van Pandora wordt voor het onderwijs. Kinderlokkers in chatboxes, verontrustende blootstelling aan porno en geweld op het internet, jonge cybernauten die zich ontpoppen tot hackers of handelaars in illegale gekopieerde software, toenemend pestgedrag via sms, groeistoornissen bij minderjarige pcverslaafden, …. De lijst van gevaren lijkt afschrikwekkend.

Gelukkig laat wetenschappelijk onderzoek een genuanceerder beeld zien. Daaruit blijkt dat jongeren vaak weerbaarder zijn dan we denken. Bovendien bestaan er tal van hulpmiddelen om problemen te voorkomen of op te lossen.

Het behoort onmiskenbaar tot de maatschappelijke taak van het onderwijs om aandacht te besteden aan kennis en vaardigheden betreffende ICT. Sinds 1 september 2007 zijn nieuwe vakoverschrijdende eindtermen voor ICT van kracht in het basisonderwijs en de eerste graad van het secundair onderwijs. Eén van deze eindtermen slaat op het veilig, verantwoord en doelmatig gebruik van ICT. Het gaat hier om een breed scala van competenties en attitudes, zoals nauwkeurig en verzorgd werken, zorg dragen voor apparatuur en software, alertheid voor schadelijke of discriminerende inhouden, enz.

Het invoeren van eindtermen is één zaak. Daarnaast is het nodig om scholen voldoende te ondersteunen zodat zij op een veilige manier van de vele didactische mogelijkheden die ICT biedt, gebruik kunnen maken. Deze publicatie wil daarbij een hulpmiddel zijn.

Ze bevat actuele informatie, concrete tips, lesmateriaal en richtlijnen over veilig ICT-gebruik op school. De publicatie is bedoeld voor leraren, directies én ICT-coördinatoren. Ze is thematisch geordend. Je kunt elk hoofdstuk apart lezen. Stukken over de schoolwebsite en de beveiliging van netwerken tegen virussen zijn allicht interessanter voor de ICT-coördinator, terwijl hoofdstukken over gezond computergebruik en schadelijke inhouden op internet voor iedereen interessant zijn.

Deze publicatie bevat ook een cd-rom met een aantal filmpjes, lespakketten en aanvullende informatiebronnen. In de verschillende hoofdstukken vind je relevante verwijzingen naar die extra's.

Na elk hoofdstuk volgen verwijzingen naar verdere informatie: referenties van softwareprogramma's, links en contactadressen waarnaar in de tekst wordt verwezen.

Wij hopen dat deze gids je mag helpen bij het uitbouwen van een veilig en kwaliteitsvol ICT-beleid op school.

.1.

WAARVOOR GEBRUIKEN JONGEREN COMPUTER EN INTERNET?

In de kinder- en jongerencultuur hebben computer en internet een centrale plaats verworven. Gemiddeld spendeert een twaalf- tot achttienjarige anderhalf uur per dag aan activiteiten op internet. 95% van alle vijftienjarigen heeft thuis toegang tot pc en internet. Meer dan vier op vijf jongeren chat minstens een keer per week. Meer dan de helft van de zestienjarigen downloadt elke week muziek of films van het internet. Technisch-instrumentele vaardigheden, zoals het maken van een website of het installeren van software, leren ze vaak op hun eentje, van elkaar of van familie…

Dat is het profiel van de huidige generatie Vlaamse jongeren. Het geeft een beeld van een generatie die opgroeide met moderne communicatietechnologie, deze volledig heeft geïntegreerd in haar dagelijkse bezigheden en over de nodige technische vaardigheden beschikt. Maar ze leerden dat niet noodzakelijkerwijze op school.

Maar jongeren gaan vaak ook heel intuïtief en soms weinig beredeneerd en kritisch om met ICT. En daar komt de school op de proppen. De meeste leraren die nu voor de klas staan, groeiden zelf niet op met ICT. Sommigen fronsen ongetwijfeld de wenkbrauwen bij het horen van “cybertermen” als games, skype, blogs, podcasts, googlen, sms’en en msn’en. Toch verwacht de maatschappij dat leraren leerlingen veilig, verantwoord en doelmatig met ICT leren omgaan.

In deze publicatie vind je een hoop tips, lesmateriaal en hulpmiddelen voor de aanpak daarvan. In dit inleidende hoofdstuk staan we stil bij de internetgeneratie. Wie zijn ze en wat doen ze?

1.1 Nieuw voor jou? Niet voor hen!

Voor je grootouders waren vliegtuigen 'nieuwe vervoermiddelen'. Voor jou al lang niet meer. Ben je een van de jongste collega's op school? Dan groeide je zelf op met computers, al hadden ze als puber waarschijnlijk nog geen permanente verbinding met het web. Ben je ouder dan dertig? Dan is de kans groot dat je het wereldwijde web pas als adolescent volwassene leerde kennen. Dan zijn pc's internet, chat, e-mail, gsm nog 'nieuwe media'. Voor je leerlingen zijn ze dat al lang niet meer.

Jongeren groeien op met gsm, sms'jes, pc in de huiskamer of het bureau van pa en ma. En als ze wat ouder zijn: in de veilige cocon van hun eigen kamer! In de kleuter- en in de lagere school staat er een computer in de klas en is er een computerlokaal waar ze klassikaal met de pc werken. Voor jouw leerlingen zijn gsm en computer vanzelfsprekend.

Jij bent opgegroeid met de telefoon. Je gebruikt hem om je emoties te delen. Je belt naar het thuisfront als je op reis bent. Waarschijnlijk heb je ook de gsm in je leven geïntegreerd als middel om extra bereikbaar te zijn.

Maar chatten? Jouw foto op een profielsite? Dat lijkt jou vreemd, misschien zelfs onecht, gevoelsarm. Maar voor jouw leerlingen hebben chatboxen, msn, e-mails, profielsites niets virtueels, het is écht. Het is hun leefwereld en hun communicatiemiddel bij uitstek.

1.2 De ICT-leefwereld van jongeren

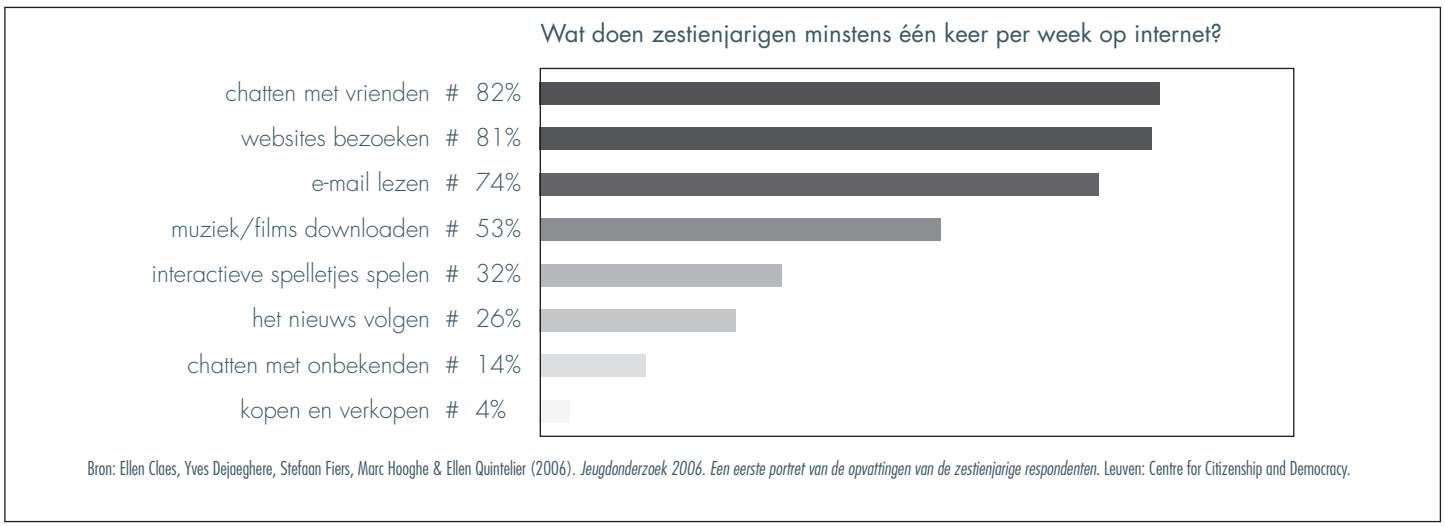
Jongeren gebruiken een computer niet op dezelfde manier als volwassenen. En kinderen van 10 doen wat anders dan pubers van 13 of adolescenten van 17. Wat doen ze allemaal op hun computer?

Volgens Tom Van Renterghem (Child Focus) kun je jongeren ruwweg in drie leeftijdsgroepen opdelen, elk met een eigen interessesfeer.

>>**Kinderen van 6 tot 10 jaar** gebruiken computers vooral als ontspanning. Ze spelen spelletjes en bezoeken websites rond kinderprogramma's op tv (Ketnet) of van hun favorieten (K3, Diddle,…).

>>**Jongeren van 10 tot 14/15 jaar** zoeken vooral communicatie en interactie met leeftijdsgenoten: zij maken gebruik van sms'jes en chatboxen bij hun zoektocht naar een eigen identiteit. En ze gamen.

>>**Vanaf de leeftijd van 14/15 jaar** beginnen ze ICT meer en meer te gebruiken zoals volwassenen: ze zoeken informatie. Toch blijven chatsessies en games vaak nog belangrijk.



Bron: Ellen Claes, Yves Dejaeghere, Stefaan Fiers, Marc Hooghe & Ellen Quintelier (2006). *Jeugdonderzoek 2006. Een eerste portret van de opvattingen van de zestienjarige respondenten.* Leuven: Centre for Citizenship and Democracy.

Chatten of msn'en

Vooral vanaf de leeftijd van 10–11 jaar willen jongeren chatten. Een chatbox is een virtuele leefruimte waar je samenkomt om te babbelen via tekstboodschappen. Die tik je in en versterk je met emoticons: :) :(:D :p :/

Volwassenen vragen zich soms af: wat doen jongeren toch urenlang in zo'n chatbox ? Ze komen uit de klas en beginnen meteen met klasgenoten te babbelen op internet. Het is de vraag die ouders en opvoeders zich ook vroeger stelden — als hun kinderen urenlang aan de telefoon hingen.

Ze kletsen gewoon. Ze lossen huistaken op en praten over wat er in de klas gebeurde. Ze vertellen over hun dromen en intiemste gedachten, of ze babbelen gewoon over niks. Als er maar contact is. Ze testen uit hoe anderen op hen reageren — een stap in hun zoektocht naar persoonlijkheid en identiteit. Chatten is ook een graadmeter voor hun populariteit: het gaat erom zo veel mogelijk chatvrienden te hebben.

De populairste chatwereld is MSN van Microsoft – vandaar 'msn'en'. MSN werd wel herdoopt tot 'Live Messenger'. Sommige chatboxen zijn volledig 'open': iedereen heeft toegang en er is geen enkele vorm van controle. Andere zijn 'gesloten': de chatters hebben zelf controle over wie ze tot hun kring toelaten. Wie op MSN wil geraken heeft een .NET-paspoort nodig.

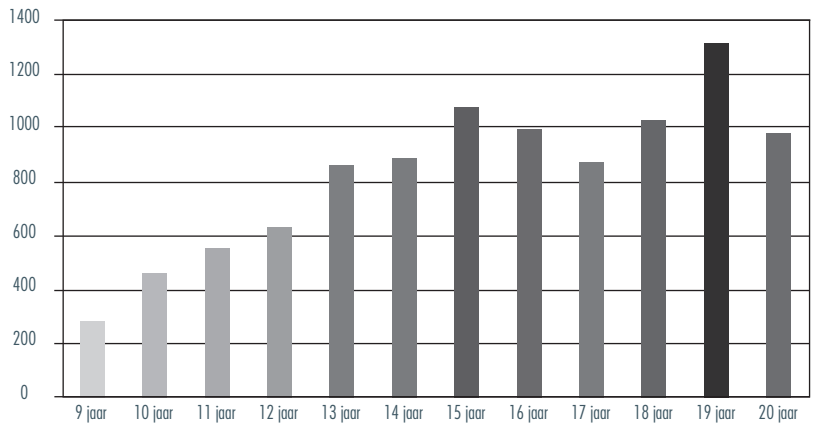
Een aantal chatboxen (zoals netlog.be) hebben moderatoren die gebruikers voor korte of lange tijd kunnen blokkeren als ze ongewenst gedrag vertonen.

> *"Thuis komen en meteen messenger aanzetten, dat is een gewoonte geworden. Al mijn vrienden en klasgenoten zitten daarop en dan kun je over schoolwerk praten. Het is handiger dan sms'en en het kost niets.*
> *Het is nog veel populairder bij mensen die jonger zijn dan wij. Ik denk dat veertienjarigen het gebruiken om contact te leggen met iemand die ze anders niet durven aanspreken. Mijn zus is elf en als ze verliefd is, gebeurt alles vooral via messenger."*
>
> Charline, 17 in De Morgen 2007–03–23

Webcam

Een webcam is een klein cameraatje dat je op de computerscherm monteert en je bewegingen opneemt zoals een videocamera. Het kost twee keer niks en behoort tot de standaarduitrusting van een multimediacomputer. Via de webcam stuur je beelden naar het internet en kun je een chat- of skypepartner zien terwijl je tekst intikt of praat.

Gemiddeld aantal minuten dat jongeren elke week internet gebruiken, volgens leeftijd



Bron: Vandebosch, Heidi, Van Cleemput, Katrien, Mortelmans, Dimitri, Walrave, Michel, *Cyberpesten bij jongeren in Vlaanderen, studie in opdracht van het viWTA*, Brussel, 2006

Surfen

Net als volwassenen surfen jongeren meestal niet in het wilde weg op het internet. Ze hebben een doel voor ogen. Ze zoeken games, software of muziek. Of hopen een prijs te winnen met een online wedstrijd. En natuurlijk gaan ze op zoek naar informatie over hun hobby of voor schoolopdrachten. Het is belangrijk dat volwassenen hen erop wijzen dat ze voorzichtig moeten zijn met het prijsgeven van informatie over hun identiteit.

Jongeren gebruiken internet als een reusachtige ongestructureerde encyclopedie. Hier ligt een belangrijke taak voor de school: leerlingen leren herkennen welke informatie betrouwbaar en valide is. Daarop gaan we later uitgebreider in.

E-mailen

Al heel jong willen kinderen graag een e-mailadres. Niet dat ze elkaar al veel berichten sturen. Maar hun vriendjes hebben er ook een. Bovendien hebben ze een e-mailadres nodig om deel te nemen aan wedstrijden van websites zoals Ketnet, Diddle, K3,…

Een e-mailadres is bovendien volledig gratis. Zeer populair bij jongeren zijn de gratis hotmail-adressen omdat ze dan meteen een .NET Passport krijgen dat hen toegang geeft tot MSN.

Downloaden

Jongeren gebruiken massaal internet om muziek (mp3-bestanden), software, foto's en filmpjes te downloaden naar hun harde schijf. De juridische aspecten bespreken we in detail verder in deze brochure.

> *"Op onze leeftijd heb je gewoon geen keuze. Je zult altijd proberen te vermijden om voor muziek te betalen. Als je supersterren ziet met gouden kettingen en gigantische wagens, dan denk je niet: "Die moet ik financieel steunen." Ik koop alleen cd's van groepen waar ik veel respect voor heb."*
>
> Jan, 17 jaar in De Morgen 2007–03–23

Websites en profielen

Een website maken? Dat is erg leuk om te doen. Je experimenteert met techniek — en zo leer je veel. En je speelt met je identiteit. Want je stelt jezelf voor aan de hele wereld. Precies daarmee zijn tieners intens bezig.

Jongeren vullen ook persoonlijke profielen in bij hun chatbox, maar ook op pure profielsites zoals MySpace, MSN Spaces, party.be, funkyplace.be, sugababes.nl en superdudes.nl. Die websites komen tegemoet aan een natuurlijke behoefte bij pubers. Ze willen luid en duidelijk verkondigen: 'Ik besta'. Zowel op websites als op profielsites publiceren jongeren vaak ook fotoalbums.

Forums en gastenboeken

Forums zijn een soort prikborden waar jongeren aan elkaar vragen stellen. Gastenboeken vind je zowel op websites van vedetten als op websites van jongeren zelf. Ook dit zijn plekken waar jongeren zich kunnen oefenen in het formuleren van hun gedachten en visies. Maar er zijn ook neveneffecten. Soms verzanden ze in scheldpartijen of dom geleuter. Forums hebben vooral waarde als ze onder leiding staan van een moderator die de gesprekken in goede banen leidt.

Fun

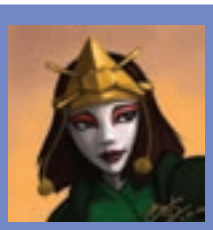
Jongeren spelen. Hoewel ze daar een ander woord voor hebben: *gamen*.

Vanaf de kleuterleeftijd zijn kinderen geboeid door computerspelletjes op cd of dvd. Als ze groter worden willen ze ook interactiviteit. Ze willen zich meten met leeftijdgenoten en zoeken naar open spelvormen op het web. Daar zitten heel communicatieve spelvormen tussen, zoals het Habbohotel (www.habbo.be) of Runescape (www.runescape.com). Daar meten kinderen zich een virtuele identiteit of avatar aan. Ze spelen en communiceren er met andere jongeren en verkennen de grenzen van hun eigen identiteit.

Sommige jongeren worden aangetrokken door games vol spanning en geweld. Studies hebben nog nooit aangetoond dat geweldspellen aan de basis liggen van gewelddadig gedrag in de reële wereld. Er zou alleen een versterkende invloed zijn bij jongeren waar het psychologisch al fout mee loopt.

Normaal zijn geweldspellen dus geen reden om je zorgen te maken: voor jongens is het een veilige manier om te experimenteren met hun gevoelens en hun grenzen te verkennen. Het is niet bedreigender dan 'soldaatje spelen'.

Zie ook www.spelletjes.be, www.hln.be/fun of www.msn.com/games voor voorbeelden van online spelletjes.



Een avatar wordt gewoonlijk gebruikt als verpersoonlijking of visualisering voor de persoon achter de computer. Het is de verschijning van een speler in de virtuele wereld. Een avatar is meestal een icoontje dat dient als identificatie op internetfora, chatprogramma's. Avatars staan meestal naast of onder de nickname van een lid.

In videogames, online games of virtuele omgevingen zoals Second Life is een avatar vaak een bewegend personage.

De term komt waarschijnlijk uit het Hindi. De naam raakte bij jongeren ingeburgerd door de Amerikaanse animatieserie Avatar. Die speelt zich af op een sprookjesversie van de aarde, sterk beïnvloed door Aziatische, Indiaanse (native American) en Inuit (Eskimo) cultuur. In deze wereld leven mensen, fantasiedieren en geesten.

Zo begin je aan je eerste sessie in Runescape. Noteer dat er meteen een knop aanwezig is om ongewenst gedrag te signaleren.

Skypen

Dit is telefoneren via internet met het VOIP-protocol (Voice Over Internet Protocol). Skype is het bekendste programma voor VOIP. Je kunt het gratis downloaden. Je belt dan via je computer volledig gratis met een gesprekspartner om het even waar ter wereld.

Het is dus ook voor volwassenen een interessant kanaal om goedkoop én met beeld te communiceren, bijvoorbeeld met familieleden of vrienden die in het buitenland verblijven — of met kinderen 'op kot'. Je hoort elkaars stem en met een webcam zie je elkaar ook. Terwijl het je niks kost, behalve eventueel de aanschaf van een koptelefoon met microfoon en webcam (en dat heb je al voor minder dan 50 euro).

Je kunt ook skypen naar vaste telefoons tegen lage tarieven. Of een speciale skype-telefoon kopen. Dan hoeft je computer zelfs niet aan te staan om goedkoop te bellen. Pas wel op als je je laptop meeneemt op vakantie en dan skypet: de internetverbindingskosten liggen dan misschien hoger dan gewone telefoontarieven.

http://www.skype.be/intl/nl/

Bloggen

Blog is een afkorting van weblog: een dagboek op internet. Niet alleen populair bij tieners, maar ook bij volwassenen. Denk maar even aan de blogs van politici waar kranten regelmatig uit citeren.

Een aantal leraren experimenteert met de educatieve mogelijkheden die blogs bieden: een eigentijdse omgeving waar jongeren leren hoe ze teksten schrijven, hun mening formuleren, een boodschap presenteren, enz. (zie ook www.edublogs.be). Een variant zijn de moblogs waarbij je tekst en foto's van op je gsm naar je weblog doorstuurt.

1.3 De taak van het onderwijs

Je hoeft geen computerfreak of fanatiek surfer te worden om jongeren te begeleiden. Je zult altijd wel leerlingen in de klas hebben die handiger zijn met het medium. Dat is geen probleem. Vraag hun hulp en advies. Ze zullen je graag helpen.

Maar wat wél nodig is, is dat ze kritisch leren omgaan met media en informatie. Er komt een massa aan informatie op hen af. Ze hebben een groot netwerk om sociale contacten op te bouwen en te experimenteren met hun persoonlijkheid. Jongeren hebben steun nodig van leraren en ouders om hen te helpen bij het afbakenen van hun grenzen en hen te behoeden voor mogelijk misbruik.

Daarom brengen we in deze brochure informatie en tips die je helpen bij die begeleidingstaak. Je leert er hoe je hen opvoedt tot WAKkere (weerbare, alerte en kritische) internauten. Zo worden ze gebruikers die letterlijk én figuurlijk 'gezond' omgaan met de krachtige mogelijkheden die ICT hen biedt.

Als leraar heb je een dubbele opdracht:

(1) Je moet ervoor zorgen dat je zelf optimaal kunt werken. Dat betekent dat je zelf weet hoe je aan betrouwbare informatie komt en hoe je jezelf beschermt tegen digitale hindernissen.

(2) Je moet je leerlingen opvoeden tot bewuste computergebruikers en internauten. Je moet ze tonen welke voorzorgsmaatregelen ze moeten nemen, hoe ze kunnen nagaan of informatie betrouwbaar is en hoe ze misbruiken kunnen vermijden.

Soms moet je zelfs de ouders van je leerlingen ondersteunen. Want natuurlijk spelen ouders een heel belangrijke rol bij de opvoeding rond ICT-gebruik.

Wakker worden

Veilig internetten draait om een **wak**kere houding. Drie principes lopen als een rode draad door deze brochure: een computer- en internetgebruiker is

weerbaar: hij dekt zich in tegen al wat veilig, efficiënt, resultaatgericht computeren in de weg staat (virussen, spam, gegevensverlies, pestgedrag,…);

alert: hij is op zijn hoede voor hackers en internetgebruikers die misbruik willen maken van de openheid en vrijheid van het web;

kritisch: hij stelt voortdurend de geloofwaardigheid in vraag van de informatie die hij op internet vindt en ziet het verschil tussen betrouwbare en onbetrouwbare informatie.

Eindtermen

Vanaf 1 september 2007 bepalen nieuwe eindtermen de ICT-doelstellingen die de school moet halen aan het einde van het (buitengewoon) basisonderwijs en de eerste graad van het secundair onderwijs. Je vindt een overzicht op http://onderwijs.vlaanderen.be/ict. Op dezelfde webpagina vind je ook het beleidsplan voor de periode 2007–2009. Daarin wordt de draagwijdte van deze eindtermen toegelicht. Deze eindtermen bieden volop aanleiding om de verschillende thema's die in deze publicatie opgenomen zijn, aan bod te laten komen in de klas.

Meer informatie

Websites met informatie

www.gezinsbond.be/veiligonline

www.saferinternet.be

Video en online games

www.pegionline.eu — site met informatie over gebruik en gevaren van online games

www.isfe.eu — site van de gaming industrie met informatie, tips, onderzoek en links naar de belangrijkste spelletjesmakers

Virtuele wereld (voorbeelden)

www.habbo.com

www.secondlife.com

.2.

BETROUWBAARHEID VAN INFORMATIE

Er staan miljoenen pagina's op internet. Over duizenden onderwerpen. Even een paar zoektermen googlen en je krijgt soms tienduizenden verwijzingen naar webpagina's. Maar hoe weet je welke informatie betrouwbaar is en welke niet?

Jongeren hebben de neiging om alles wat ze op internet lezen voor waarheid aan te nemen. Je moet ze leren het kaf van het koren te scheiden. Sluitende regels bestaan daar niet voor, maar er zijn wel een aantal elementen die je informatie geven.

Het trainen van leerlingen in de correcte interpretatie, evaluatie en verwerking van bronnen is een belangrijke stap naar de realisatie van de nieuwe eindtermen voor ICT.

Criteria

De school is de plaats bij uitstek om jongeren te leren informatie op zijn waarde te beoordelen. Dat is niet alleen een doelstelling van ICT, maar van elk (algemeen) vak. Leer je leerlingen een website beoordelen aan de hand van een reeks criteria:

(1) Is de website objectief of 'gekleurd'?

(2) Is de bron betrouwbaar?

(3) Is de auteur bekend? Heb je informatie over de organisatie, het bedrijf… die de validiteit van de informatie waarborgt? Is de informatie up-to-date of dateert de laatste aanpassing van verschillende jaren geleden?

(4) Wat is het doel? Wil de auteur werven, reclame maken of informeren? Is de informatie correct en volledig?

2.1 Is de website objectief of 'gekleurd'?

In een aantal gevallen zal het webadres (de URL of Uniform Resource Locator) je al heel wat kunnen vertellen.

Webadressen als ugent.be, ua.ac.be, kuleuven.be, vub.be verwijzen duidelijk naar universiteiten en dan weet je dat de informatie inhoudelijk een hoge betrouwbaarheidsgraad heeft. Surf je naar de website van een overheidsdienst? Dan zullen er geen leugens op staan.

Surf je naar adressen van politieke partijen? Dan weet je dat je partijgekleurde informatie krijgt. Die kan best heel correct zijn en terzake, maar ook een welbepaalde visie vertolken.

Alle websites met als achtervoegsel '.com' zijn in principe eigendom van bedrijven, die met '.org' van organisaties. Daarmee weet je dus in feite niets. Evenmin als met websites die een landcode als laatste deel hebben, zoals '.be', '.nl',…

Deze website lijkt op het eerste gezicht heel betrouwbaar. De URL wekt vertrouwen: 'www.martinlutherking.org' en de titel ook: 'A True Historical Examination'. Onderaan de pagina wordt eerst nog meer vertrouwen gewekt met 'Civil Rights Library'….

Tot je de onderste regel leest: 'hosted by Stormfront', de hedendaagse Ku Klux Klan.

2.2 Is de bron betrouwbaar?

Daarna moet je naar andere elementen zoeken. Met de website over Martin Luther King waar je schermafdrukken van vindt op deze pagina, bewijs je de leerlingen online dat ze goed uit hun doppen moeten kijken.

2.3 Is de auteur bekend?

Tilde

Vind je websites met in de URL een tilde (~) gevolgd door een voornaam en/of familienaam, dan ben je waarschijnlijk bij de website van een individuele gebruiker terechtgekomen. Dan hangt de betrouwbaarheid af van de persoon die de pagina's maakte.

Dat is ook zo als de URL begint met een voornaam, familienaam of nickname, zoals 'bollekeuh.startje.com'. Daarnaast zijn er de

duidelijk herkenbare websites die gratis startpagina's aanbieden zoals everyoneweb.com of geocities van Yahoo. Dit soort gratis websites is meestal ook herkenbaar aan de advertenties waarmee de aanbieders aan inkomsten geraken.

Foute omleiding

Let op voor websites die je bereikt als je een foutje typt in de URL. Als je bijvoorbeeld 'www.simens.be' intikt in plaats van 'www.siemens.be', kom je op een webpagina vol advertenties, zonder enige verwijzing naar wie erachter zit.

Vaak zitten daar personen achter die hopen om die homonieme URL tegen een flink bedrag te verkopen aan het bedrijf of de dienst die door de omleiding wordt benadeeld. Soms zijn het ook echte hackers die je omleiden naar een tijdelijke website waar ze proberen aan je persoonlijke gegevens te komen of geld te incasseren (meer hierover bij 'phishing').

De eigenaar van het foutgespelde Siemens zit niet om een grapje verlegen (telefoonloze draad!), verdient vast een stuivertje aan de advertenties en stelt de domeinnaam te koop (zie rechts bovenaan).

WhoIS

Whois is de term die internationaal gebruikt wordt om informatie over de eigenaar van een domeinnaam op te vragen. Belgische domeinnamen worden beheerd door de vzw DNS. Op de bijhorende website www.dns.be kan je gegevens opvragen van de eigenaar en DNS provider van elke .be domeinnaam.

Contactinformatie

Een andere waardemeter is de aanwezigheid van informatie over de eigenaar van de website. Staan er duidelijke gegevens over het bedrijf of de organisatie? Zijn er namen, adressen, telefoonnummers voor contactname? Vind je een gebruikersovereenkomst of privacyverklaring?

Als je geen van die elementen aantreft op een website, dan moet je argwaan koesteren. Een schoolvoorbeeld van duidelijke communicatie rond de website is die van de Katholieke Universiteit Leuven waar je onderaan elke pagina de naam van de auteur vindt (en als je die aanklikt, krijg je contactgegevens zoals e-mailadres en telefoonnummer), de datum van de laatste update, een disclaimer en ook een link naar de webmaster.

2.4 Wat is het doel?

Kom je terecht op een website van een tabaksfirma met studies die aantonen dat roken echt niet zo schadelijk is? Dan wijst dat duidelijk op belangenvermenging. Beweert een website dat je met hun methode gegarandeerd op zes maanden van je tabaksverslaving verlost bent? En kost die enkele honderden euro? Dan moet je wel elders bevestiging zoeken van de efficiëntie van die methode.

Lesmateriaal

Op de website van Klascement.net vind je een lesfiche en een test over het evalueren van internetinformatie. De leerlingen kunnen met de test zelf evalueren of ze voldoende kritisch naar websites kijken. Surf naar http://digitaalso.klascement.net en selecteer lesfiche 11 "evalueren van websites".

De website www.webdetective.nl biedt eveneens lesmateriaal aan: een interactieve cursus, oefening en een online checklist voor het beoordelen van websites.

.3.

VEILIG COMMUNICEREN, E-PRIVACY EN E-COMMERCE

In dit hoofdstuk gaan we dieper in op enkele aspecten van communiceren via ICT. Eerst staan we stil bij de eigenheid van communiceren via internet, de zogenaamde nettiquette. Vervolgens komen zaken als spam en e-privacy aan bod. Tenslotte wordt stilgestaan bij een aantal consumentgerelateerde aspecten, zoals aankopen via internet. De inhoud van dit hoofdstuk is heel belangrijk in functie van de eindterm: leerlingen kunnen ICT gebruiken om op een veilige, verantwoorde en doelmatige manier te communiceren.

3.1 Nettiquette

Wat etiquette doet voor de gewone omgangsvormen, doet nettiquette voor de digitale communicatie. En dan bedoelen we zowel e-mail als forums of chatboxen, internettelefonie, blogs en foto's of filmpjes van jezelf en anderen. Sleutelwoorden daarbij zijn beleefdheid en respect.

Opvoeden tot nettiquette valt voor alle onderwijsvormen onder de eindterm: 'leerlingen kunnen ICT gebruiken om op een veilige, verantwoorde en doelmatige manier te communiceren'.

Bezin voor je verzendt

Digitale communicatie heeft twee belangrijke kenmerken: de snelheid en (met uitzondering van contacten met webcam) de afwezigheid van lichaamstaal. Helemaal nieuw is dat niet. We kennen die al decennia bij de telefoon. Je kunt in een opwelling van woede de hoorn grijpen en iemand de huid vol schelden of koud terechtwijzen. Ook dan zie je niet hoe de persoon reageert (gebaren, oogcontact, lichaamshouding,…). Je brengt enkel nuances aan met een beperkte set van non-verbale communicatie (stemintonantie, spottende toon,…).

Deze kenmerken doen zich bij digitale communicatie ook voor. Je krijgt een bericht in je mailbox. Je wordt boos en typt meteen een felle reactie. Even snel nalezen, een druk op de verzendknop: je e-mail is onherroepelijk weg.

Tip: denk driemaal na voor je een bericht verzendt. Als een e-mail je boos maakt, laat dan even bezinken en bekoelen. Als je boosheid verantwoord is, kan je die nog kenbaar maken, misschien via een minder anoniem medium. Bedenk ook dat e-mail gemakkelijk te bewaren en door te sturen is en niet steeds op het beste moment bij de ontvanger terechtkomt.

Enkele vuistregels voor correct e-mailverkeer:

(1) doe niet mee aan kettingbrieven of rampberichten.

(2) neem enige reserve in acht bij het doorsturen van e-mails.

(3) maak een onderscheid tussen beantwoorden en beantwoorden aan allen

(4) Schrijf korte en bondige teksten, zonder te vervallen in telegramstijl die aanleiding kan geven tot misverstanden.

(5) Geef een bericht een duidelijk onderwerp mee, zodat de essentie voor de ontvanger meteen duidelijk is.

(6) Antwoord nooit meteen als je boos of geërgerd bent.

(7) Wees voorzichtig met grappen en sarcasme, gebruik liever emoticons zoals :-) het lachebekje en ;-) de knipoog.

(8) Gebruik geen hoofdletters als het niet nodig is. Ze zijn schreeuwerig en onbeleefd.

Jongeren: geen echte naam

Belangrijk is dat jongeren geen e-mailadres aanmaken waarin ook hun familienaam voorkomt. Als ze dan ook nog ergens hun gemeenteplaats achterlaten als informatie, zijn ze immers heel gemakkelijk opspoorbaar (bv. via de 'Witte Gids' op internet of 1207).

Sommige deskundigen adviseren om zelfs de eigen voornaam niet te gebruiken, maar wel een 'nickname'. Wijs oudere kinderen er ook op dat ze geen adres maken in de sfeer van 'hardcoresletje', 'geilegozer', 'hotlips',… Dat type adres is een uitnodiging voor seksueel getinte toenaderingspogingen van vreemden.

3.2 Spam

Spam is ongewenste reclame die je via e-mail ontvangt. De term 'spam' vindt zijn oorsprong bij de stand-up comedians van Monty Python? Die maakten een sketch over een koppel dat een taverne binnenstapt voor een lekkere hap. Helaas, bij elke schotel op het menu zit 'spam' — een merknaam voor Amerikaans varkensvlees in blik. Wat het koppel ook probeert, altijd weer kiepert de kok er een schep spam bovenop. Precies wat nu gebeurt met je mailbox: je krijgt stapels berichten die je

niet wenst. Reclame voor geneesmiddelen, penis- en borstvergrotingen, porno, enzovoort. Maar ook bedelbrieven.

Op je brievenbus thuis kleef je een sticker als je geen reclame wilt. Maar wat doe je met je mailbox? Iedereen heeft minstens af en toe last van spamberichten (zie ook technisch luik voor leraren).

En je hebt als leraar vast een lijstje van e-mails die je liever niet krijgt. Zo verwacht je allicht niet dat leerlingen de dag voor toets of examen nog vragen komen stellen over de leerstof, of hun beklag doen over medeleerlingen. Iedereen heeft zijn lijst van reclameboodschappen die hij niet wenst te ontvangen.

Hello,

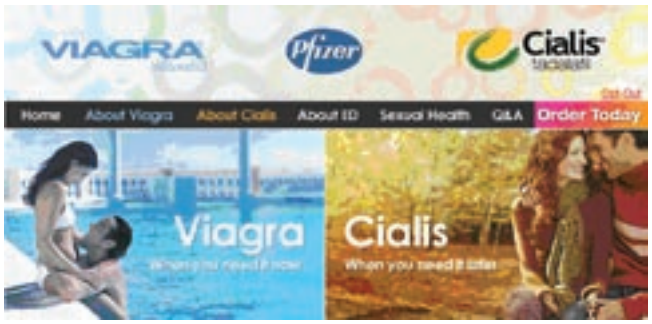
Now you can order Authentic Viagra directly from Pfizer.

Here: http://www.youmeetmyfriends.info

All prices are tax/vat free and free same-day world-wide shipping also included.

--
hfmsmomnmgkqlumtmllsjojqjjfsjljf

Typische spammail voor Viagra en andere producten. Natuurlijk brengt Pfizer zijn product niet zo aan de man.



De website ziet er zo uit. De logo's bovenaan zijn niet aanklikbaar. Nog een bewijs dat het hier om namaak gaat. De echte truc zit in de 'opt-out': daar vragen ze je e-mailadres als je geen post meer wilt ontvangen. Vul je dat in? Dan hebben ze pas een adres dat ze kunnen overstelpen met spam.

Handel preventief

Een volledige bescherming? Neen, dat lukt je niet. Maar je kunt de hoeveelheid spam indijken. Hoe je software kunt inschakelen om de hoeveelheid spam te verminderen, dat lees je in het technisch luik voor leraren.

Maar je kunt ook preventief ingrijpen. In de eerste plaats door goed uit je doppen te kijken als je op een website formulieren invult, producten aankoopt of je inschrijft voor diensten. Meestal staat daar ergens een zinnetje in piepkleine lettertjes dat je vraagt of het bedrijf je ook informatie mag sturen over andere producten of van bevriende handelaars. Het bedrijf of de organisatie moet je uitnodigen om het vakje aan te vinken als je later informatie wenst te krijgen ('opt-in' op basis van de wet van 11 maart 2003).

Opt-in voor de nieuwsbrief van onderwijswebsite Klascement.

Je kunt je e-mailadres ook op de 'Robinsonlijst' laten opnemen. Dan heeft hetzelfde effect als de sticker op je brievenbus: je krijgt geen ongewenste mails van bedrijven die lid zijn van het Belgisch Direct Marketing Verbond (BDMV). Het is geen beveiliging tegen andere spam.

Als een bedrijf of organisatie je dan e-mails of nieuwsbrieven begint te sturen, heb je altijd het recht om je uit te schrijven. Bonafide verzenders hebben onderaan hun bericht een link die je moet aanklikken om automatisch uit te schrijven. Is die er niet? Dan kun je een e-mail sturen naar het bedrijf of de organisatie en vragen dat zij je uit hun bestanden schrappen. Je hebt trouwens ook op het recht op inzage in de gegevens die een bedrijf of organisatie over jou bijhoudt en het recht om correcties te doen uitvoeren.

Wat doe je nog meer?

(1) Zorg dat je e-mailadres niet op een website staat. Doe je dat toch? Gebruik dan een beschermde vorm (bv. Info(at-teken)vlaanderen.be — zie tips in technisch luik voor ICT-coördinatoren).

(2) Wil de directeur dat elke leraar met zijn e-mailadres op de website van de school staat? Bespreek dat op een personeelsvergadering en zoek de goede aanpak.

(3) Gebruik een specifiek gratis e-mailadres telkens je op een website je e-mailadres moet intikken (bv. om informatie te krijgen, voor een spelletje, om geschenken, prijzen te winnen,…).

(4) Wil je e-mails ontvangen van leerlingen? Kies dan een webmailadres dat je niet voor normale persoonlijke post gebruikt. Ten eerste bepaal jij dan zelf wanneer je de berichten leest (want je moet expliciet naar een website surfen om ze te lezen). Ten tweede bescherm je je tegen spam die eventueel via leerlingen op jou afkomt.

Hoe komen spammers aan je adres?

Een ander facet is de pure ongewilde spam. Die wordt verstuurd door personen of bedrijven die op volledig illegale wijze aan je e-mailadres komen. Maar hoe vinden die jouw adres?

Er zijn niet alleen 'bedrijven' of personen die spam verzenden. Er zijn er ook die geld verdienen met het verzamelen van e-mailadressen. Hoe doen ze dat?

(1) Spamrobots zoeken wereldwijd websites af op zoek naar e-mailadressen (die ze herkennen aan het at-teken (@) gevolgd door een domeinnaam). Als je e-mailadres vermeld staat op je persoonlijke website of op die van je school, je vriendenclub of sportvereniging, kun je in spamlijsten komen.

(2) Kettingmails gaan vaak niet alleen naar de contactpersonen uit het adresboek, maar ook naar een spamcentrale.

(3) Zoekmachines testen 'waarschijnlijke' e-mailadressen (bv. info@domeinnaam, contact@domeinnaam) af en versturen een e-mail met een bevestigingsvraag. Lukt die? Dan zijn ze zeker dat het een correct adres is.

(4) Je hebt spamberichten met de vraag om een link naar een website te volgen voor meer informatie. Volg je die link? Dan gaat je e-mailadres mee.

(5) Virussen of spyware nestelen zich op een computer, verzamelen alle e-mailadressen uit het adresboek en sturen die door naar de verzamelaar.

Voorbeeld spamtrucs

Hello,
Best Pric at e Today,
S rg AVE on your Med le ic mj ation!

Viagr jt a $3.35
Ci nm alis $3.75
Va mo lium $1.35
Xan mn ax $1.45
A gf mbien $2.90
S lb oma $1.15
and many other.

Vi fk sit our site

Als je een spammail kopieert, merk je de trucs die afzenders gebruiken om voorbij spamfilters te komen. Elk 'spamfiltergevoelig' woord wordt hier onderbroken door extra tekens. In je mail zie je die niet staan, maar ze zitten wel in de code.
Achter de hyperlink zit bovendien een 'raar' websiteadres: *http://safiymaneal.superpezheadrecords.com/*. Als je een week of zo later nog eens naar dat adres surft, werkt de URL niet meer. Spamverzamelaars gebruiken immers meestal erg tijdelijke domeinnamen.

Heb je last van veel spammails van eenzelfde bron? Op de website van de federale spamsquad vind je de adressen waar je klacht kunt indienen (rubriek: hoe handelen?). Daar vind je een lijst met meldpunten voor spam of ander misbruik via internet. Je kunt je probleem ook online melden op de website www.ecops.be.

3.3 E-privacy

Websites vragen heel vaak naar persoonlijke gegevens. Het is belangrijk dat jongeren van jongs af leren om zich af te vragen of het wel zinvol dat je dat om de haverklap doet. Vaak stelt een bedrijf of organisatie die vraag om je achteraf informatie (of reclame) toe te sturen.

Respect voor de privacy is in onze maatschappij een belangrijk goed. Iedereen wenst respect voor zijn of haar privéleven. Het internet is een medium dat erg open is. In een telefoonboek staan ook privégegevens maar het internet maakt de ontsluiting van namen, e-mailadressen,… veel gemakkelijker. Tik maar eens je eigen naam in op een zoekrobot. Wedden dat er verschillende websites zijn waar je naam of je e-mailadres op voorkomt?

De beschikbaarheid van privé-gegevens biedt opportuniteiten voor mensen met slechte bedoelingen. Soms is dat eerder onschuldig zoals het versturen van ongewenste reclame (spam), soms gaat het om regelrechte schendingen van de privacy, zoals het ongevraagd verspreiden of publiceren van foto's.

Waarschuw vooral jonge kinderen

Beoordelen of een website wel met goede bedoelingen naar je persoonlijke gegevens vraagt, is helemaal niet vanzelfsprekend voor jonge kinderen. Zij zijn meestal erg argeloos en bereid om het even wat vrij te geven in ruil voor een geschenkje.

De raad die je aan kinderen kan geven is: vraag raad aan een volwassene voor je persoonlijke gegevens invult op een website: adres, telefoonnummers,… Vul zeker nooit bank- of kredietkaartgegevens in. Niet op een website, niet in een chatbox, niet in een e-mail. En — we herhalen het — ook nooit een wachtwoord.

Minderjarigen hebben natuurlijk zelf geen kredietkaart. Het is belangrijk dat ze beseffen dat ze ook de gegevens van de kaart van hun ouders, oudere broer of zus niet mogen invullen zonder toestemming.

Dat advies communiceer je als leraar best ook naar de ouders, want ook hier moeten ouders en school aan hetzelfde zeel trekken. Suggereer aan de ouders dat ze beter een afzonderlijk e-mailadres voor de kinderen aanmaken, dan en alias van het e-mailadres dat aangeboden wordt door de provider.

Minderjarigen, minder rechten?

Een meerderheid van de websites die hoofdzakelijk bestemd zijn voor kinderen en tieners verzamelt persoonsgegevens van de jonge bezoekers zonder hun privacyrechten te respecteren. Hoewel zo'n 8 op de 10 websites persoonsgegevens verzamelen, hebben daarvan slechts 4 op de 10 een privacy statement. Bovendien is deze wettelijk verplichte informatie vaak onvolledig.

Zo'n acht op de tien onderzochte websites (82,4%) verzamelen op één of andere manier persoonsgegevens. Daarbij wordt gevraagd naar de naam (81%), naar contactgegevens als e-mail (87%), adres (54%), telefoonnummer (32%) of gsm-nummer (19%), maar ook naar persoonskenmerken als leeftijd (37%), geslacht (15%), hobby's (7%), nationaliteit (6%) of studies (5%).

Uit: Prof. dr. Michel Walrave (2005) *Cyberkids' e-Privacy. Minderjarigen, minder rechten.*

Echt geheim

Het is belangrijk dat je leerlingen zo jong mogelijk inprent dat een wachtwoord absoluut en 100% geheim moet zijn. Ze mogen het niet verklappen aan hun lief, vrienden, chatkameraden, broer of zus.

Ervaring leert dat de helft van de kinderen in de lagere school hun wachtwoord niet onthouden. Dan kan het nuttig zijn dat

de ouders en/of de leraar het (tijdelijk) ook kennen. Anders blokkeren leerlingen soms de toegang tot hun e-mail. Begin bij erg jonge kinderen met een niet te lang woord dat bestaat uit de eerste letters van woorden uit een zin die ze zelf opstellen. En sluit de zin af met een uitroepingsteken of vraagteken. Dat helpt kinderen om het te onthouden.

Je schrijft een wachtwoord niet op. Dat is ook enorm belangrijk voor elke leraar op school. Als leerlingen jouw netwerkwachtwoord aan de weet komen, hebben ze meteen toegang tot alle informatie en gegevens waar de ICT-coördinator of directeur hen wil van weg houden. Denk maar aan toets- en examenvragen, punten en rapporten, persoonlijke gegevens van je collega's.

Duidelijke afspraken

Als school of individuele leraar maak je best duidelijke afspraken met leerlingen over e-mail in het begin van het schooljaar zoals:

- **(1)** met welk soort vragen ze je mogen mailen;
- **(2)** hoeveel tijd je jezelf gunt om hun e-mails te beantwoorden (bv. binnen de twee schooldagen);
- **(3)** of ze je nog vragen mogen stellen de dag(en) voor een toets of examen.

Dit soort duidelijke afspraken zijn ook wenselijk als de school gebruik maakt van een elektronische leeromgeving (Smartschool, Blackboard, eloV, Moodle…).

Ik wil anoniem blijven

De wet op de bescherming van de persoonlijke levenssfeer bepaalt dat wie op internet persoonlijke gegevens verzamelt, aan de gebruiker moet meedelen wat hij met die gegevens wil doen. Hij mag die gegevens ook alleen verzamelen als de gebruiker ondubbelzinnig zijn toestemming geeft en de gegevens noodzakelijk zijn voor het uitvoeren van de overeenkomst tussen beide partijen. Hij moet ook uitdrukkelijk vermelden hoe en waar de gebruiker verzet kan aantekenen tegen het gebruik van zijn gegevens, hoe hij inzage krijgt en correcties kan laten doorvoeren.

Wie wat rondsurft, ontdekt al snel dat meerdere websites die regels met de voeten treden. Wat doe je dan als je toch die gratis software, dat rapport,… wilt downloaden? Niemand belet je om fictieve gegevens in te vullen. Niet alle websites controleren het werkelijke bestaan van een e-mailadres zoals aaa@abc.be.

Vul persoonlijke gegevens alleen in als je zeker bent van de goede bedoelingen van de vragende partij. En let er dan nog op dat je je niet tegelijk abonneert op nieuwsbrieven of toestemming geeft om je persoonlijke gegevens te gebruiken voor ongewenste marketingdoeleinden, indien je dat niet wenst.

3.4 Foto's op de schoolwebsite

Scholen zitten voortdurend gevangen tussen:

- de wens van ouders om foto's van kinderen op de website te vinden, zeker als die op bos-, zee- of sneeuwklassen zijn;
- en de wet op de bescherming van de persoonlijke levenssfeer.

Toestemming vereist

De wet zegt heel helder en duidelijk: je hebt de uitdrukkelijke toestemming nodig als je foto's publiceert waarop personen herkenbaar in beeld komen. De regel is dus: het mag niet, tenzij je toestemming hebt of de personen niet herkenbaar zijn. Plaats zeker nooit privégegevens zoals naam of e-mailadres bij foto's.

Als een minderjarige de leeftijd heeft bereikt waarop hij zelf kan beslissen (in rechtstaal: 'de leeftijd van onderscheidingsvermogen'), vraag je zijn toestemming. De rechter bepaalt autonoom of een jongere dat onderscheidingsvermogen volgens hem al bereikte. De rechtspraktijk leert dat rechters dit criterium al snel aanvaarden. De toestemming (ook) vragen aan de jongere zelf is dus een goede praktijk.

Bij foto's van andere minderjarigen heb je de toestemming van de ouders nodig — en van beide ouders als ze gescheiden zijn. Meerderjarigen geven natuurlijk zelf toestemming.

De Commissie voor de Bescherming van de Persoonlijke Levenssfeer stelt in haar advies dat "de individuele en voorafgaandelijke toestemming (dus een echte opt-in) vereist is om geschillen te vermijden". Een algemene toestemming van de ouders is dus onvoldoende. Bovendien kan de betrokkene zijn toestemming op elk moment intrekken.

Minderjarige met onderscheidingsvermogen beslist zelf

"Wanneer we te maken hebben met minderjarigen, dient een onderscheid te worden gemaakt tussen minderjarigen met en zonder onderscheidingsvermogen. Om dit te beoordelen gaat de rechtbank voor elke concrete handeling na of de minderjarige tot een redelijke beoordeling van zijn belangen in staat kan worden geacht. Er is geen officiële leeftijdsgrens waarop zij worden geacht een onderscheidingsvermogen te hebben ontwikkeld. Indien de minderjarige nog geen onderscheidingsvermogen heeft ontwikkeld, zal de toestemming moeten worden verkregen van de wettige vertegenwoordigers, dus de ouders of voogden. Indien blijkt dat de minderjarige wel een onderscheidingsvermogen heeft ontwikkeld, wordt door een meerderheid in rechtspraak en rechtsleer aangenomen dat de toestemming van de minderjarige volstaat."

Evi Werkers, Legal Researcher bij het Interdisciplinair Centrum voor Recht en Informatica (ICRI-K.U.Leuven)

Uitzonderingen

Als een klas betoogt voor vrede of tegen geweld, kan een leerling of zijn ouders er zich niet tegen verzetten als je daarvan foto's publiceert. In principe is ook geen voorafgaande instemming nodig wanneer de afbeelding werd gemaakt op een openbare plaats. Foto's gemaakt tijdens een schoolreis waarbij eerder de omgeving het onderwerp van de opname is dan de leerlingen, kunnen dus zonder problemen op de website een plaatsje krijgen, zeker als de leerlingen niet herkenbaar zijn. De rechtspraak vindt dat een klasfoto hier niet onder valt, want daar behoudt elke leerling zijn 'persoonlijk karakter'.

Er is ook een verschil tussen een foto in de schoolkrant en op de website. De schoolkrant heeft een beperkte verspreiding. De website is wereldwijd voor iedereen toegankelijk.

Tip: plaats geen namen van leerlingen bij de foto. Want met naam én foto is het gemakkelijker te achterhalen wie wie is en verhoogt het risico op misbruik.

"De toestemming voor het publiceren van een foto moet op een specifieke en nadrukkelijke wijze worden bekomen. Een handtekening die een algemene toelating inhoudt in het begin van het schooljaar die terzelfder tijd andere activiteiten dekt van de leerlingen, is niet voldoende. Het te ondertekenen document moet op een nauwkeurige wijze: verwijzen naar de soort(en) foto('s) die zullen verspreid worden op het internet en naar het doel van deze verspreiding; de toelating vragen voor elke type van publicatie dat in overweging wordt genomen zodat de ouder zich bijvoorbeeld kan verzetten tegen het online zetten van het portret van zijn kind, terwijl hij wel de verspreiding van de klasfoto accepteert."

Advies nr. 38/2002 van 16 september 2002 van de Commissie voor de bescherming van de persoonlijke Levenssfeer over de bescherming van de persoonlijke levenssfeer van leerlingen op internet.

Stilzwijgend akkoord volstaat niet

Een clausule in het schoolreglement die vermeldt dat foto's van uitstappen, speciale activiteiten,… op de website kunnen terechtkomen, maar dat ze meteen worden verwijderd als de leerling of de ouders dat vragen, is onvoldoende. De Commissie voor de Bescherming van de Persoonlijke Levenssfeer stelt in een advies duidelijk dat dit niet conform de wetgeving is. De school moet de toestemming vooraf vragen en niet na het publiceren.

Vanzelfsprekend geldt die regel ook voor elke leraar. Heb je bezwaar tegen jouw foto op de schoolwebsite (of tegen een bepaalde foto)? Meld het aan de directie en vraag dat de webmaster die foto verwijdert. De directie kan je niet verplichten om je foto online te zetten. Dat geldt trouwens ook voor schoolbrochures of folders. Ook daar mag een leraar of leerling alleen met foto komen mits uitdrukkelijke toestemming.

> *"In het fotoalbum en op de website verschijnen met regelmaat foto's van de activiteiten die plaatsvinden in onze school. Indien je bezwaar hebt tegen een foto, zal deze onmiddellijk verwijderd worden."*
>
> Uittreksel uit privacyverklaring van een school.

Een clausule als deze is onvoldoende.

3.5 E-commerce

Webwinkels zijn in opmars. De omzet voor België lag in 2006 rond 2 miljard euro en blijft stijgen. Ook jongeren kopen steeds vaker op internet. En komen soms bedrogen uit. Ze kopen bijvoorbeeld iets online met betaling 'onder rembours'. Als de postbode weg is, blijkt het pakje alleen krantenpapier te bevatten. Of het bestelde product wordt nooit geleverd.

Adviseer je leerlingen om altijd eerst goed op de website te kijken of de webwinkel wel betrouwbaar is. Is er een pagina met contactgegevens? Publiceert de handelaar zijn verkoopvoorwaarden en garantiebepalingen? Weet je waar je terecht kunt als er iets misloopt? Kun je ook telefonisch contact opnemen? Is er een fysiek adres?

Geef je leerlingen de goede raad niet met een hyperlink uit een reclamemail naar een webwinkel te surfen, maar het adres zelf in te typen (zie ook onder 'phishing').

Tips voor veilig kopen op het net

Het Europees Centrum voor de Consument somt een aantal eenvoudige basisregels op.

(1) Koop alleen op betrouwbare sites die de verplichte informatie geven.

(2) Lees de algemene verkoopsvoorwaarden (als deze beschikbaar zijn) vooraleer je bestelt. Print ze en bewaar ze.

(3) Kijk op de site welke waarborgen de handelaar biedt en hoe je van een eventuele dienst na verkoop kan genieten.

(4) Bevestig je bestelling nooit voordat je zeker weet dat je de totale prijs kent (inclusief btw, verpakkings- en verzendingskosten).

(5) Print en bewaar je bestelbon.

(6) Betaal liefst niet op voorhand, maar na ontvangst van je bestelling. Indien dit niet mogelijk is, betaal dan met een kredietkaart.

(7) Labels geven niet altijd de zekerheid dat de webwinkel te vertrouwen is. Informeer eerst bij de uitgever van het label.

Veilig betalen

Je loopt natuurlijk het minste risico als je online bestelt en je bestelling zelf afhaalt bij de verkoper of op een leveringspunt en daar betaalt. Of onder rembours aan de postbode.

Betaal je online met je kredietkaart? Kijk dan of er onderaan op de statusbalk van je browser een icoontje staat met een gesloten hangslot of een sleuteltje: dat staat symbool voor een beveiligde site. Die herken je meestal ook aan het internetadres (URL) op de adresbalk: dat begint met 'https' in plaats van 'http'.

Het is niet normaal als de verkoper, na je online bestelling en betaling, een e-mail stuurt met de vraag om je bestelling of betalingsgegevens te bevestigen. Beantwoord zulke mail niet. Neem rechtstreeks contact op met de verkoper, telefonisch of via het e-mailadres op de website.

Lesmateriaal

De federale overheidsdienst Economie lanceerde een campagne tegen consumentenbedrog via gsm en internet. Die richt zich vooral op de jonge consument. Je vindt er basisinformatie, nuttige tips, enz.

Leerlingen kunnen er ook hun consumentengedrag testen met een online quiz. Die quiz vind je ook in de brochure 'Kopen op het internet' van het Europees Centrum van de Consument. Je vindt die op de cd-rom bij deze publicatie. De brochure geeft naast algemene tips ook uitleg bij de juiste antwoorden op de quizvragen.

3.6 Meer informatie

Bescherming persoonlijke levenssfeer
www.e-privacy.be — daar kun je studie 'Cyberkids' e-privacy' downloaden.
www.privacycommission.be — (let op: je moet een tijd wachten voor het doorklikmenu verschijnt op de homepagina)
www.saferinternet.be
www.web4me.be — deze website is bedoeld voor leerlingen tussen 14 en 18 jaar jaar oud.

Aanbevelingen
mineco.fgov.be/information_society/enterprises/providers_internetguide/Providers1_nl-01.htm
www.privacycommission.be

Spam
www.spamsquad.be
www.ecops.be
www.internet-observatory.be

e-commerce
www.economie.fgov.be/e-prevention.htm — info, tips en 3 quizen bedoeld voor jongeren
www.eccbelgie.be — de brochure en quiz staan integraal op de cd-rom bij deze publicatie
www.oivo.be — Het OIVO (Onderzoeks- en Informatiecentrum van de Verbruikersorganisaties) biedt regelmatig informatie aan over e-commerce en consumenten bescherming.
www.consumentenbedrog.be

.4.

SPEELPLAATS ZONDER TOEZICHT

"Niemand laat kinderen zonder toezicht achter in een speeltuin. Scholen organiseren altijd toezicht op de speelplaats. Maar op internet surfen kinderen vanaf heel jonge leeftijd zonder enige begeleiding", zegt Erika Frans van vzw Sensoa. Je behoedt leerlingen op de speelplaats voor vechtpartijen, pesterijen,… Je houdt er in het oog dat waaghalzerij niet tot ongelukken leidt. Je helpt ze de straat oversteken. Leer ze ook veilig surfen.

Concreet gaan we in dit hoofdstuk in op schadelijke inhoud op internet, met een focus op seksuele inhoud, racisme en discriminatie.

4.1 Interactieve seks

Onderzoek

Een onderzoek uit 2006 van de Rutgers Nisso Groep bij 10.000 jongeren in Nederland toont duidelijk aan dat jongeren op internet bezig zijn met seks. Het televisieprogramma *Koppen* en de krant *Het Nieuwsblad* organiseerden in februari 2007 een steekproef bij 547 Vlaamse jongeren, in samenwerking met diezelfde Rutgers Nisso Groep en Child Focus. De resultaten van dit onderzoek wijzen erop dat de Vlaamse jeugd overwegend gezond reageert op seks op internet. Een jongere op vier kreeg het voorbije jaar wel eens een seksuele getinte vraag. Maar de grote meerderheid (7 op 10) vindt dit niet tof en slechts 23% antwoordt ook op dit soort vraag. Als ze antwoorden, gebeurt dit omdat ze de gesprekspartner vertrouwen of er verliefd op zijn (56%). Vier jongeren op tien reageren omdat ze dat spannend of leuk vinden.

Acht procent van de jongeren maakte het voorbije jaar iets mee op seksueel gebied wat ze 'vervelend' vinden. Acht jongeren op honderd kregen ook de vraag om iets seksueels te doen voor de webcam. 80% had die vraag liever nooit gekregen. Twee ondervraagde jongeren toonden ook effectief geslachtsdelen. Dat waren jongens uit de leeftijdsgroep van 17 tot 18 jaar die dat 'spannend' vonden. Acht meisjes (1,5%) zetten het voorbije jaar wel eens sexy foto's van zichzelf online.

Tieners weten van wanten

"De meeste tieners hoef je ook niets meer te vertellen over de risico's op internet. Ze zijn digitaal gepokt en gemazeld. Die netwijsheid hebben ze opgedaan door vallen en opstaan en door verhalen die ze elkaar vertellen. Ze maken geregeld dingen mee die niet prettig zijn, maar hoe sterker ze in hun schoenen staan, hoe beter ze ermee kunnen omgaan en hoe minder ze zelf dit soort ervaringen negatief beoordelen", schrijven Pardoen en Pijpers in hun boek *'Verliefd op internet'*.

Betekent dit dat je als leraar gewoon de ogen mag sluiten en tot de orde van de dag overgaan? Geenszins. Het onderwijs heeft een opdracht om jongeren op te voeden tot bewust en gezond omgaan met seksualiteit — ook op internet. Onderzoek toont ook aan dat lager opgeleide meisjes vaker seksuele verzoeken krijgen en erop ingaan dan hoger opgeleide meisjes.

> *"De anonimiteit van het internet helpt jongeren bij het aanleren van communicatie. Vandaag zijn er veel die minder afhankelijk worden van hun uiterlijk. Normaal wordt communicatie immers beïnvloed door kledij, voorkomen, enz. Er is een heel groep jongeren die daar geen deel aan nam. Dankzij de anonimiteit van internet ben je veel gelijker met de anderen. Er zijn meer jongeren die nu durven, die proberen en die op die manier met elkaar communicatie leren."*
>
> Kinderpsychiater dr. Peter Adriaenssens in de VRT-uitzending *"Koppen"* van 27 maart 2007

Geen paniek

Wat je niet moet doen? Je door de media angst laten aanpraten. Natuurlijk gebeuren er ongelukken in de digitale wereld. Precies zoals in de gewone wereld. De digitale wereld betekent voor heel wat jongeren een andere en bredere waaier van mogelijkheden tot experimenteren. Alles gebeurt sneller, is anoniemer, toegankelijker. Het Vlaamse jeugdonderzoek toont dat 82% van de jongeren regelmatig chat. De kansen voor experimenten liggen dus voor het grijpen.

Als leraar moet je jongeren mee motiveren om grenzen te stellen en risico's te vermijden. "Pubers kunnen een pésthekel hebben aan de regels en grenzen die volwassenen hen opleggen, maar diep in hun hart hebben ze er ook ontzettend behoefte aan," stellen Justine Pardoen en Remco Pijpers in *'Verliefd op internet'*.

Jongeren moeten beseffen dat ze zich in feite op straat begeven. Daar gaan ze ook niet naakt rondlopen of in een uitdagende outfit staan dansen, laat staan masturberen. Toch laten ze zich daar soms voor een webcam toe verleiden. Gewoon omdat ze thuis op hun kamer zitten, waar ze zich veilig voelen. Maar die beslotenheid stopt als de beelden naar de provider vertrekken. In volgende hoofdstukken gaan we dieper in op deze gevaren.

Welke seksualiteit?

Jongeren worden steeds vaker geconfronteerd met de beeldvorming: 'op seksueel vlak moet je voor alles openstaan'. Dat gebeurt niet alleen op internet, maar het is ook daar de trend. Die beeldvorming legt een enorme druk op de jongeren. Je eigen grenzen stellen? Daarvoor moet je al wel heel sterk in je schoenen staan. De school heeft een belangrijke rol om die stereotiepen te helpen doorbreken.

Leraren kunnen jongeren ondersteunen bij het opbouwen van een persoonlijke levensvisie waarbij ze zelf hun grenzen bepalen. Ze moeten leren aanvoelen waar ze zich goed bij voelen en wanneer ze een brug te ver dreigen te gaan.

Verleiders hebben tijd

De media overspoelen je regelmatig met reportages van journalisten die zich in een chatbox uitgeven voor een jong meisje. Na een paar uur chatten hebben ze dan steeds een paar afspraakjes op zak met mannen die seks met hen willen hebben.

Dat geeft een misleidend beeld. Vooral omdat je al heel lang zult moet zoeken voor je een jongere vindt die al na een paar minuten chatten een afspraakje vastlegt met een wildvreemde (man). Zo dom zijn jongeren gelukkig niet.

Het gevaar schuilt hem eerder in langdurige contacten. De ervaring leert dat de meeste oneerbare voorstellen niet van onbekende volwassenen komen, maar van leeftijdsgenoten, familie of vrienden. En een geruststelling: de meeste jongeren gaan er niet op in.

Echte verleiders nemen hun tijd. Maandenlang hebben ze regelmatige contacten met mogelijke slachtoffers. Ze nestelen zich dan vooral in de rol van begrijpende, ondersteunende, empathische gesprekspartner die zo anders is: hij begrijpt alles, vindt alles goed, motiveert. Zo wint hij vertrouwen en pas dan zet hij een volgende stap.

> *"Sommige mannen pakken dat heel fijnzinnig aan. Ze komen heel lief over, ze zorgen ervoor dat je hen begint te vertrouwen. En ze zijn heel geloofwaardig. Ze kunnen echt tot in de puntjes antwoorden op je vragen."*
>
> Jolien, 16, in *Het Nieuwsblad* van 27 maart 2007

Zo gebeurt het ook in de niet-digitale wereld. Wie jongeren wil verleiden, zoekt naar jongens en meisjes die zich onbegrepen voelen, een emotioneel tekort ervaren. Heel langzaam wordt een afhankelijkheidsrelatie opgebouwd waar ze nog moeilijk uitkunnen.

Opgepast met webcam

Het is belangrijk dat je als leraar jongeren duidelijk waarschuwt voor de gevaren van een webcam. Het lijkt zo onschuldig. Je toont je lichaam aan dat meisje of die jongen waar je smoor op bent. Je bent zo vol vertrouwen… En het lijkt onschuldiger en veiliger dan je lichaam te tonen als je liefje echt naast je staat. Je denkt er zelfs niet aan dat die beelden vastgelegd worden voor altijd. Dat ze straks kunnen worden getoond aan iedereen. De liefde raakt uit. Een nieuwe, nog bekorender partner verschijnt aan de horizon. En er blijft er eentje ontgoocheld en jaloers achter. En dan gebeurt het: de beelden worden misbruikt voor haatmail of cyberpesten.

Of erger nog. De persoon die de jongere verleidde om zich letterlijk bloot te geven, had nooit goede bedoelingen. Hij wou alleen beeldmateriaal om de jongere onder druk te zetten om verder te gaan. Dan volgen de dreigementen: ofwel kom je naar een afspraak op mijn kamer/in mijn huis, ofwel verstuur ik de beelden naar je ouders. Van kwaad naar erger.

Er is dus maar één goede raad voor jongeren: 'Toon nooit je naakte lichaam, masturbeer *nooit* voor een webcam.' Een gelijkaardige boodschap stuur je als leraar ook naar de andere partij: neem nooit webcam-beelden op. En verspreid ze zeker nooit. Het is niet alleen

kwetsend voor anderen. Je overtreedt bovendien de wet (schending van privacy) en je kunt daarvoor gestraft worden.

Een vijftienjarige jongen getuigt: *"Ik ben opgepakt vanwege het verspreiden van meerdere naaktfoto's van een minderjarige. Ik word strafrechtelijk vervolgd en heb er spijt van. Ik wist niet precies wat ik deed… maar ja, gebeurd is gebeurd, ik zal het niet meer doen en licht anderen er ook over in het niet te doen. Ik vertel ze dat het nergens voor nodig is om die foto's op internet te zetten en dat je iemand anders daar alleen maar veel pijn kunt mee doen."*

Bron: Pardoen & Pijpers, *Verliefd op internet.*

"Het zijn vooral mannen die je vragen om je uit te kleden voor de webcam. Dat weet toch iedereen. We zijn dat ondertussen al zo gewoon dat we er niet meer van schrikken." — Tiny, 17

"Het wordt gewoon belachelijk. Elke week krijg ik wel enkele berichten in de aard van: "Sta jij ook zo heet?" of "Ik wil seks met je". Ik lees ze zelfs niet meer. Ik smijt ze weg zonder ernaar te kijken en ik denk: weer zo'n zielig aard achter een computer die niet gewoon op café kan gaan om een meisje te leren kennen." — Jolien, 16

Citaten uit *Het Nieuwsblad* van 27 maart 2007

Betrap je leerlingen erop dat ze foto's of filmpjes doorsturen? Of meld een leerling (of zijn/haar klasgenoten) dat compromitterende beelden de ronde doen? Overleg met directie en CLB. Onderzoek samen of contact met politie aangewezen is.

Nooit alleen naar een live date

Het heeft geen zin jongeren aan te zetten om nooit een afspraak te maken met iemand die ze op internet ontmoeten. Uit een ontmoeting in chatrooms of via e-mail kunnen immers ook waardevolle liefdesrelaties groeien.

Toch is enige waakzaamheid wel geboden. Waarom? Ten eerste ben je nooit zeker van de echte leeftijd van de persoon met wie je afspreekt. De digitale identiteit is niet controleerbaar. Ten tweede kan een chatvriend heel lief zijn op internet, maar bij een ontmoeting veel verder willen gaan dat jij wenst. Een jongere beperkt de risico's aanzienlijk als zij/hij niet alleen gaat, en bovendien ouders/leraar/vertrouwenspersoon op de hoogte brengt van de afspraak.

"Toch vind ik de voordelen van internet groter dan de nadelen. Ik heb aan het internet mijn vriend te danken. Ik had die jongen in het echt een keer gezien, maar ik had nog geen woord met hem gewisseld. Via de chat zijn we aan de praat geraakt en zo zijn we een koppel geworden. Babbelen is nu eenmaal makkelijker via internet dan in het echt. Ik ben opener via internet."

Tatjana, 18 in *Het Nieuwsblad* van 27 maart 2007

Enkele basisregels

Natuurlijk blijven ook de basisregels voor veilig internetten van toepassing:

(1) geef geen privégegevens zoals eigen naam, namen van familieleden, vrienden, telefoonnummers, huisadres, naam van de school, e-mailadres, waar je ouders werken, kredietkaartgegevens;

(2) geef het wachtwoord van je profielsite, e-mail, chat,… niet door aan anderen;

(3) meld elke intimidatie aan de beheerder van de site of een vertrouwenspersoon (ouder, leraar,…).

4.2 Expliciete beelden

Pornografie en seksueel misbruik van kinderen zijn prominent aanwezig in de aandacht van media en maatschappij. Hoe beschermen we jonge kinderen en pubers tegen expliciete en ongewenste beelden? Hoe vermijden we dat ze in handen vallen van

kinderlokkers? Hoe vermijd ik dat mijn zoon of dochter ingaat op de vraag van een chatmaatje en zich uitkleedt voor de camera, misschien zelfs masturbeert? Met het risico dat die beelden straks de wereld rondtoeren.

De media spelen daar handig op in met verhalen van journalisten die via chat al na een paar uur surfen werden uitgenodigd voor een afspraakje in de stad. Maar niet daar schuilt het gevaar: meestal komen de verleiders uit de kennissenkring, zijn het mensen die de jongeren al een heel tijd kennen en met wie ze een vertrouwensrelatie opbouwden.

Kinderen zoeken voor hun spreekbeurt naar informatie. En ze krijgen pornografische beelden op hun scherm geprojecteerd. Ze surfen naar websites met foto's van zwaar verminkte lijken. Of googlen naar websites waar je kunt zien hoe Sadam Houssein wordt opgeknoopt. Kun je dat — alvast op school — verhinderen? Hoe doe je dat? Hoe bereid je jongeren voor op choquerende beelden? Hoe scherm je ze af van racistische peptalk?

Pornografie is meer dan puur beelden. Die wereld vertrekt van foute en ongewenste verwachtingspatronen. Het is een wereld waar alle meisjes (en vrouwen) staan te springen om met één of meer kerels in bed te duiken, liefst met zoveel mogelijk standjes. Het toont seks zonder liefde, het is fysieke opwinding om de fysieke opwinding. En dus moet je steeds verder gaan. Jongeren worden zo in een verarmde, stereotiepe wereld gelokt die bovendien extreem vrouwonvriendelijk is. Meisjes zijn er puur lustobjecten en jongens pompende seksmachines.

Er is heel veel pornografie op internet. Gewoon omdat het een erg lucratieve markt is. Het bewijs? In 2005 werd de domeinnaam sex.com verkocht voor 14 miljoen euro en in mei 2007 verwisselde domeinnaam porn.com voor 7 miljoen dollar van eigenaar.

4.3 Pedagogische aanpak

Onderzoek toont aan dat kinderen tussen 12 en 14 jaar het minst vaak met hun ouders praten over seks. En dat is nu precies de leeftijd waarop ze het meest beïnvloedbaar zijn en dus het meest begeleiding nodig hebben. Precies in die leeftijdsgroep (laatste jaar basisonderwijs en eerste graad secundair) is het belangrijk dat je als leraar de kloof dicht rijdt.

Want het zijn precies jonge pubers die het minst gewapend zijn tegen seksuele uitnodigingen. Meer nog: twaalf- en dertienjarigen doen zich graag ouder voor dan ze zijn. En op internet is dat veel eenvoudiger dan in het gewone leven! Precies daarom is deze leeftijdsgroep het meest kwetsbaar: ze stellen zich ongedekt op en hebben geen wapens. Maak die leeftijdsgroep duidelijk dat ze voorzichtig moeten zijn en grenzen stellen. Leer ze hoe ze dat kunnen doen.

Lessen

Op het internet is er heel veel materiaal dat je als leraar kunt gebruiken rond deze thematiek. Child Focus is actieve partner in het Europese netwerk 'Safer Internet' en stuurt de website Clicksafe.be. In Vlaanderen is de organisatie Action Innocence actief met vorming voor leraars en ouders. Sensoa ondersteunt leraren met een interactief lespakket. Er is de website van Mijn kind Online in Nederland. Voor de jongsten is er de brochure en website 'Als een visje door het net', een goed vertrekpunt voor discussie.

Veel scholen bieden in hun elektronische leeromgeving of op hun website een positieve selectie aan van websites die ze leerrijk vinden. Vanaf tien jaar kun je ook de Jeugdwebwijzer van het Vlaams Centrum voor Openbaar Bibliotheekwezen (VCOB) op de website http://webwijzer.jeugdbib.be. Voor adolescenten is er http://webwijzer.bibliotheek.be. Zij verzamelen per thema een inventaris met links naar zinvolle websites. Je bent dus zeker dat je leerlingen surfen naar websites waarvan de inhoudelijke waarde is getoetst aan kwalitatieve normen. Je kunt er dus gerust in zijn dat je leerlingen niet op ongewenste websites terechtkomen. Die toegangspoort tot inhoudelijk waardevolle informatie voor jongeren bestaat al een tijdje, maar kreeg recent een facelift.

Filters

Internetspecialisten zoeken al jaren naar filters die ongewenste inhoud tegenhouden. Er zijn op dit ogenblik een hele reeks commerciële producten op de markt. Maar werken die? En wensen we die?

Hoe werkt een internetfilter?

'Blacklisting': je blokkeert ongewenste internetadressen (URL's). Die zitten in lijsten die de producenten bijhouden en regelmatig aanvullen.

'Whitelisting': je kunt enkel surfen naar goedgekeurde sites.

'Content filtering': je blokkeert zoektochten naar ongewenste woorden. Zo kun je instellen dat de browser de zoekmachine blokkeert als je 'borsten' intypt, of woorden als 'penis', 'vagina', 'pijpen',…

Meestal gaat het om een combinatie van deze technieken.

Voor- en nadelen

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 in de eerste plaats best leren zwemmen.

Die aanpak willen we ook toepassen op ongewenste inhoud op internet. Het is belangrijk dat de school kinderen leert ongewenste inhoud te vermijden of meteen weg te klikken. Want thuis staat er misschien geen filter op hun browser. Trouwens, laat tieners maar even aan het werk en ze vinden thuis snel hun weg om de filters heen.

Nadelen van filters

(1) Je leert de leerlingen niet hoe ze met ongewenste beelden moeten omgaan.

(2) Een filter is nooit 100% waterdicht of up-to-date.

(3) Als je blokkeert op woorden, blokkeer je tegelijk ook zinvolle inhoud. Je kunt leerlingen geen werkjes meer laten maken over poesjes, seksualiteit, doodstraf, ziekten zoals borstkanker,…

(4) Commerciële producten richten zich op een Engelstalige markt en die collecties trefwoorden zijn niet altijd bruikbaar in een Nederlandstalige context.

(5) Pornomakers linken hun websites ook creatief aan heel onschuldige woorden. Bij een zoektocht naar 'lief', krijg je meteen op de eerste pagina hits een link naar: 'lief en zacht blondje wil je verwennen'. En die stuurt je door naar de 'uitgebreidste escortsite'. Daar is geen enkele filter tegen opgewassen…

(6) Filters dagen jongeren uit om ze te omzeilen. Vaak slagen ze daar ook moeiteloos in.

Voordelen van filters

(1) Filters kunnen zinvol zijn voor heel jonge kinderen, tot de tweede graad lager onderwijs.

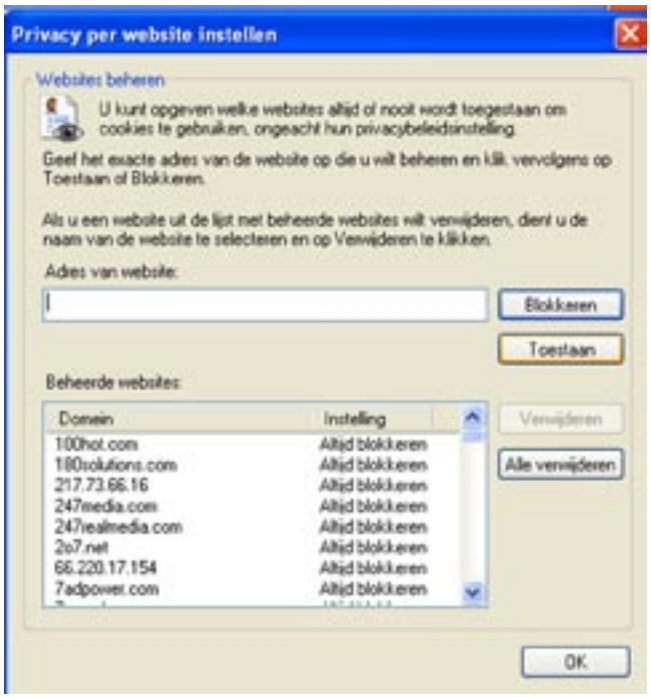
(2) Ook in het secundair onderwijs kunnen filters diensten bewijzen, met name filters die ongewenste websites blokkeren in de klaslokalen.

(3) Filters werken alleen als ze het resultaat zijn van afspraken waar alle collega's zich aan houden. Anders lijden ze tot onvrede in het team. Het is ook logisch dat de school dan — bijvoorbeeld in het schoolreglement — toelicht waarom zij voor die optie kiest.

De Europese Unie deed een vergelijkende test van de bestaande filters. Je kunt de resultaten raadplegen op: www.sip-bench.eu.

Gratis filter

In nieuwe browserversies zit de mogelijkheid van een URL-filter ingebouwd. Microsoft bouwt een aantal geblokkeerde adressen standaard in zijn Internet Explorer in. Kies in het menu 'Extra'



de rubriek 'Internetopties > Privacy' en klik daar de snelkoppeling naar 'websites' aan (zie schermafdrukken op deze pagina).

Daar krijg je een lijstje met automatisch toegevoegde URL's. Je kunt er zoveel websiteadressen aan toevoegen als je zelf wilt. Bij een test van internetfilters door de organisatie Filtra in het voorjaar van 2007 prijkt de 'Parental Control' van Windows Vista trouwens op de derde plaats qua efficiëntie.

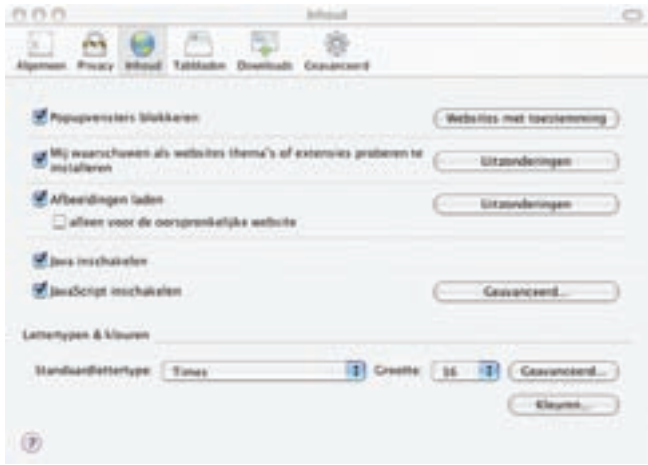
Pop-ups

Heel wat pornografisch materiaal kwam vroeger op je scherm terecht via pop-ups. Bij het laden of verlaten van een webpagina, wordt een extra venster geopend. De ene website riep de andere te voorschijn tot je hele scherm krioelde van het naakt. Nu is automatische pop-upblokkering een standaardoptie in de meeste internetbrowsers.

Tegenwoordig maakt pop-upblokkering deel uit van de beveiliging van een browser bij standaardinstallatie. Als je toch pop-ups wilt, moet je ze meestal expliciet activeren. Is de blokkering uitgeschakeld? Dan is een klikje voldoende om ze opnieuw te activeren. In Internet Explorer selecteer je in het menu 'Extra' de optie 'Pop-upblokkering' en kiest om ze in te schakelen.

In Firefox

In Firefox klik je in het menu "Extra" op Opties > Inhoud



Hier kan je de optie "Pop-upvensters blokkeren" aan- of afvinken. De knop "Uitzonderingen" brengt je naar een lijst websites die je betrouwbaar acht en die toestemming krijgen om pop-ups automatisch weer te geven.

Onderhoud van deze lijst spreekt voor zich: je kan een betrouwbare website aan de lijst toevoegen, een website individueel of in groep verwijderen.

Internet explorer

In Internet explorer selecteer je in het menu 'Extra' de optie 'pop-upblokkering' en kiest om ze in te schakelen.

Als je dan een bonafide website bezoekt die met pop-ups werkt, verschijnt er onder de adresbalk een waarschuwingsbalkje. Dat verwittigt je dat een pop-up werd geblokkeerd. Als je op dat balkje klikt, kun je kiezen om de pop-ups tijdelijk toe te staan, of om pop-ups van de actieve website altijd toe te staan. In dat laatste geval wordt de URL automatisch opgenomen in een lijstje van websites die pop-ups op je scherm mogen afvuren.

Let op: heel wat pc-banking toepassingen en internetwinkels werken alleen als je op die websites pop-ups wel toelaat. Die voeg je dan eventueel zelf toe aan de lijst van websites die pop-ups mogen activeren. Klik daarvoor de optie 'Instellingen' aan in het deelmenu voor pop-upblokkering.

4.4 Racisme en discriminatie

Even strafbaar als seksueel misbruik zijn racisme en discriminatie.

Drie wetten

De Belgische rechtspraak beschikt over drie wetten in de strijd tegen racisme en discriminatie, ook op het web:

(1) de antiracismewet van 30 juli 1981 bestraft bepaalde door racisme of xenofobie ingegeven daden;

(2) de antidiscriminatiewet van 25 februari 2003 bestrijdt discriminatie;

(3) de negationismewet van 23 maart 1995 bestraft het ontkennen, minimaliseren, rechtvaardigen of goedkeuren van de genocide tijdens de Tweede Wereldoorlog door het Duitse nationaalsocialistische regime.

Een sleutelbegrip in al deze wetten is 'aanzetten tot': de eerste twee wetten verbieden dat iemand aanzet tot discriminatie, segregatie, haat of geweld tegen personen of groepen op grond van bepaalde kenmerken zoals (zogenaamd) ras, etnische af-

stamming, seksuele geaardheid, handicap, gezondheidstoestand en geslacht. Met 'aanzetten tot' bedoelt de wetgever onder meer taal- en communicatieve uitingen die aansporen, aandrijven, ophitsen, aanmoedigen, aanstoken, oproepen en provoceren tot reacties of het plegen van feiten.

Voor eigen deur

In de eerste plaats is een school verplicht erover te waken dat er geen racisme of discriminatie voorkomt op de eigen media. Dat betekent dat racisme en discriminatie taboe zijn in schooltijdschriften, op muren en klaslokalen. Maar ook op websites, in discussiefora, e-mails en berichten binnen het schoolnetwerk of elektronische leeromgeving.
Ontdekt de webmaster, een leraar of leerling toch negationisme, discriminerende of racistische taal op het eigen netwerk? Dan moeten ze onmiddellijk actie ondernemen om die te laten verwijderen.

Het is ook mogelijk dat het Centrum voor Gelijkheid van Kansen en Racismebestrijding melding krijgt van strafbare feiten. Dan neemt dit Centrum contact op met de school (net zoals ze dat doet met een webmaster of internetservice provider) en vraagt om ervoor te zorgen dat de gewraakte passages zo snel mogelijk verdwijnen. Gebeurt dit niet? Dan kan het Centrum klacht indienen bij de gerechtelijke instanties.

Het kan nuttig zijn om de regels voor internetgebruik duidelijk zichtbaar in het PC-lokaal op te hangen en daarin op te nemen dat het bezoeken van sites en het posten van berichten met uitingen van racisme, xenofobie, negationisme en discriminatie verboden zijn.

Hallo iedereen,

Ik wil jullie verwittigen voor een bende Marokkanen die op de parking van UGC en van Metropolis wat verminkings-praktijken verrichten. Ik wil niet racistisch klinken door te zeggen dat het Marokkanen zijn maar deze keer kan ik er echt niet onderuit om het te zeggen...
Dit is echt geen grap, ik ga jullie nu dingen vertellen die echt gebeurd zijn en dit nog maar een paar weken geleden!

Een vrouw die in't stad werkte, zette haar auto altijd in de parking van de UGC. Op een avond rond 5u, zoals elke werkdag, ging ze haar auto halen om naar huis te gaan. Er zat daar een groepje Marokkanen wat onnozel te doen en toen ze de vrouw zagen zijn ze erop afgestapt. Ze hebben haar wat zitten dreigen en vroegen haar dan «EEN GLIMLACH OF VERKRACHTING» ge moogt kiezen... De vrouw wist niet goed wat ze daarmee bedoelden maar heeft dan voor een glimlach gekozen. Ze hebben haar gezicht verminkt door met een mes haar mond open te snijden tot bijna aan haar oren.

Een paar weken geleden ging een vriendin van iemand die ik goe ken naar Metropolis met haar vriend. Ze was haar GSM in de auto vergeten en is ie dan alleen gaan halen. Ze heeft JUIST HETZELFDE meegemaakt...een groep Marokkanen wilde haar GSM en hebben haar ook gevraagd wat ze wou «EEN GLIMLACH OF VERKRACHTING». Daar zij ook niet wist wat er ging gebeuren heeft ze voor een glimlach gekozen. Ook zij is nu verminkt in haar gezicht! Zij is nog maar 20 jaar!
Metropolis wou deze slechte reclame niet en heeft een grote som geld betaalt zodat ze niets aan de pers zou vertellen!

Ik vind persoonlijk dat de mensen mogen weten wat er aan de hand is en dat ze weten wat er gebeurt als ze zich in zo'n situatie terechtkomen! De mensen moeten verwittigd worden!!

Dit is echt GEEN GRAP!!! Dit is serieus!!!

Wil jij de mensen die je kent ook verwittigen? Stuur deze mail dan naar iedereen door die je kent...Het kan jou ook overkomen dus denk eraan voor je deze mail gewoon delete!

En ik zeg het nog eens: DIT IS GEEN GRAP!!! DIT IS EEN PAAR WEKEN GELEDEN ECHT GEBEURD!!!!

Mail verzonden in april 2003. De feiten beschreven in dit bericht, bleken na onderzoek volledig fictief te zijn.

Bron: *Delete Cyberhate. Racisme en discriminatie op het internet.* (2006) Uitgave van het Centrum Voor Gelijkheid van Kansen en Racismebestrijding

Bron: *Delete Cyberhate. Racisme en discriminatie op het internet.* (2006) Uitgave van het Centrum Voor Gelijkheid van Kansen en Racismebestrijding

Dialoog

Als een school laakbaar gedrag vaststelt bij een leerling, gaat zij best een gesprek aan met de betrokkene. Bij een overtreding van de bepaling in het schoolreglement, is een duidelijke sanctie vereist. Wat wettelijk strafbaar is, kan en mag een school niet oogluikend toestaan.

Het is ook belangrijk dat de school aan de leerling duidelijk maakt dat het hier gaat om gedrag dat de maatschappij kan bestraffen (er staan gevangenisstraffen op van acht dagen tot een jaar). Veel jongeren beseffen dit immers niet.

Nadeel van discussiefora

Moeilijker is het natuurlijk om weblogs en discussiefora met racisme en discriminatie te weren. Die kunnen overal zitten.

Heeft de school eigen discussiefora? Dan is het belangrijk dat die worden gemodereerd. Niet alleen op racistische inhoud natuurlijk, ook op cyberpesten en seksuele intimidatie. Daarom is een grondige discussie in de school nodig voor je discussiefora opent. Een hanteerbaar algemeen principe is dat een discussieforum alleen kan binnen een klasgroep of voor een vak waarbij de leraar het forum intensief opvolgt en modereert. Dan kan het uitgroeien tot een belangrijk didactisch hulpmiddel. Maar een open forum heeft weinig zin en kan aanleiding geven tot ongewenste situaties.

4.5 Meer informatie

Onderzoek van de Rutgers Nisso Groep in Nederland:
http://www.rutgersnissogroep.nl/Onderzoek_seks_en_internet

Websites met informatie en lesmateriaal
www.clicksafe.be
www.saferinternet.be
www.childfocus.org
www.gezinsbond.be/veiligonline bevat o.a. een aantal interessante instructiefilmpjes
www.actioninnocence.be
www.sensoa.be (het interactieve lessenpakket vind je integraal op de bijgevoegde cd-rom)
www.web4me.be richt zich tot leerlingen van 14–18 jaar oud

De brochure Als een visje door het net vind je op http://extra.msn.be/safeinternet/www/nl/index.asp

Informatie over internet filters
www.sip-bench.eu — Resultaten van Europese test van internetfilters
http://www.filtra.info — Franstalige testbank verbonden aan Action Innocence
www.ictopschool.net/infrastructuur/publicaties/uitgaven/filter/index.html

Kinder- en jeugdbrowser
Jeugd — webwijzer.jeugdbib.be
Adolescenten — webwijzer.bibliotheek.be

Boeken
Justine Pardoen en Remco Pijpers, *Mijn Kind Online. Hoe begeleid je je kind op internet*, Uitgeverij SWP 2005
Justine Pardoen en Remco Pijpers, *Verliefd op internet. Over het internetgedrag van pubers*, Uitgeverij SWP 2006

Racisme
www.cyberhate.be (de publicatie vind je integraal op de bijgevoegde cd-rom)

Meldpunten

Algemeen, federale politie (Federale Computer Crime Unit) — www.ecops.be
Meldpunt racistische en discriminerende inhouden op internet (CGKR) — www.cyberhate.be
Meldpunt kinderporno (Child Focus) — www.stopchildporno.be

.5.

CYBERPESTEN

Cyberpesten (pesten via internet of gsm) is pesten. Maar dan in het kwadraat. Jongeren ervaren het als erger en bedreigender. Ze vinden dat het nog meer dan gewone pesterijen in hun leven ingrijpt.

Volgens een onderzoek dat de Universiteit Antwerpen uitvoerde in opdracht van het Vlaams Instituut voor Wetenschappelijk en Technologisch Aspectenonderzoek (viwta), is één jongere op tien het slachtoffer van een cyberpester. Ongeveer één tiende van de jongeren was betrokken bij frequent cyberpesten: 3,3% was enkel slachtoffer, 5% was enkel dader en 2,6% was zowel dader als slachtoffer.

Wat maakt cyberpesten erger? Het zijn vooral twee factoren: cyberpesten laat een jongere nooit los en het gaat heel vaak om een één-éénrelatie tussen pester en slachtoffer. Gewoon pesten eindigt aan de huisdeur. Cyberpesten loopt verder. De hele avond door en zelfs 's nachts is er de dreiging van hatelijke sms'jes of mms'jes. De pester kan opduiken in een chatroom of doorgaan met het sturen van kwetsende e-mails.

Pesten op school is heel sterk een groepsgebeuren. Je hebt de pester, maar die heeft vaak makkers die haar/hem helpen en aanmoedigen. Het slachtoffer heeft soms klasgenoten die troosten of steun geven. En er zijn de toeschouwers: leerlingen die vaak niet weten welke kant te kiezen. Bij cyberpesten gaat het vaak om één jongere die het leven voor een andere tot een hel probeert te maken. Soms kijkt de halve wereld mee. Dat maakt het ook extra bedreigend: het slachtoffer krijgt het gevoel dat iedereen weet en ziet wat er gebeurt en hoe hij in zijn hemd wordt gezet.

5.1 Wat is cyberpesten?

Cyberpesten kan veel vormen aannemen. Van telefoontjes midden in de nacht, tot regelrechte scheldpartijen en bedreigingen. Wie het eerste hoofdstuk las, beseft hoe belangrijk chatten en msn'en zijn voor jongeren. Daarom precies ervaren ze het als een vorm van pesten als een leeftijdsgenoot hen blokkeert en uit hun groep bant.

> *"Een jongen uit mijn klas heeft 'ik wil seks' op het intranet van onze school gepost, samen met mijn mailadres, én een advertentie over mij geplaatst op een seks-site. Ik wist van niets,"* vertelt Annekien (14) die zélf moderator is op een profielensite. *"Ik kreeg al snel geile mails, en op school werd ik uitgemaakt voor hoer en slet. Het heeft drie weken geduurd voor die jongen toegaf dat hij het was. 'Ik verveelde mij', was zijn uitleg. Hij heeft zich nooit geëxcuseerd en is ervan af gekomen met strafstudie. Ik vind dat onrechtvaardig, want ik krijg nog elke dag reacties — 'waar en wanneer schatje?' — en op school bekijken veel leerlingen mij nog altijd scheef. Nu ik uit eigen ervaring weet hoe degoutant cyberpesten is, probeer ik anderen nog meer af te raden om zichzelf tijdens het chatten en in hun profiel bloot te geven."*
>
> Bron: Maks!

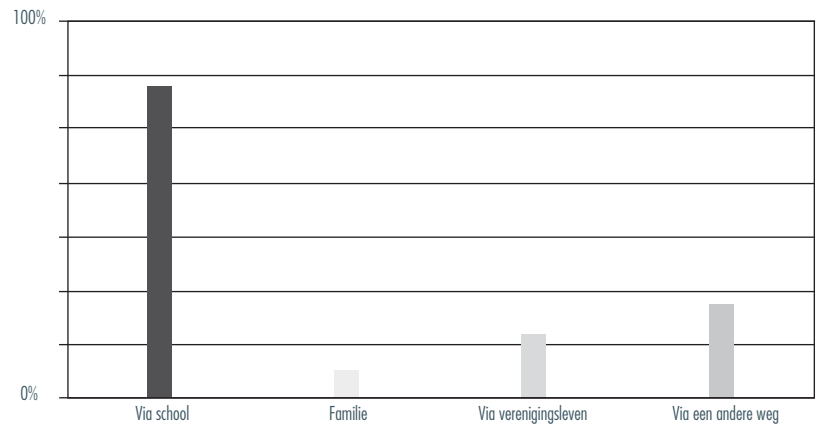
> *"Uiteindelijk moést ik het wel aan mijn ouders vertellen want ik kwam soms wenend thuis van school of zat te beven aan mijn computer,"* zegt Nick (14). *"'t Is niet alleen via msn dat ze achter mij aan zaten, ik kreeg ook scheld-sms'jes en dreigtelefoons. 'Wie zijt ge', vroeg ik. 'Ik ben uw ergste nachtmerrie', zei een vervormde stem en legde de telefoon neer. Sindsdien ben ik veel voorzichtiger met vriendschap in het echte leven en op msn. Ik hoor nieuwelingen eerst uit voor ik ze toevoeg."*
>
> Bron: Maks!

Vanwaar kent een jongere de persoon die hem pestte?

De onderzoekers van viWTA vroegen de jongeren of ze in aanraking gekomen zijn met pesten via het internet of de gsm. Eén op tien jongeren antwoordt dat hij slachtoffer is geweest, en (bijna) twee op tien dat ze dader en drie op tien dat ze getuige zijn geweest van cyberpesten.

Tijdens de drie maanden voor het onderzoek was 61,9 % van de jongeren slachtoffer, 52,5% dader, en 76,3% getuige van minstens één vorm van mogelijk kwetsende internet- of gsm-praktijken.

Ongeveer één tiende van de jongeren was betrokken bij frequent cyberpesten: 3,3% was enkel slachtoffer, 5,0% was enkel dader en 2,6% was zowel dader als slachtoffer.



Bron: Vandebosch, Heidi, Van Cleemput, Katrien, Mortelmans, Dimitri, Walrave, Michel, Cyberpesten bij jongeren in Vlaanderen, studie in opdracht van het viWTA, Brussel, 2006

Gepeste jongeren kenner de dader meestal van op school (82,2%).

Cyberpesten

Bij cyberpesten zal de pester zich meestal beroepen op een veel grondiger kennis van computers en internet. Het ultieme dreigement is vaak: pas op of ik hack je pc/e-mailadres/msn-account zodat je niet meer kunt participeren aan de online community. Het is de dreiging met het absolute isolement, het klinkt voor de jongere precies zoals: 'als je nog eens je kop buiten de deur steekt, hak ik hem af'.

> *"Leerlingen kennen mijn e-mailadres. Zo ben ik snel bereikbaar als ze vragen hebben en soms mailen ze hun huiswerk. Enkele weken geleden werden plots haatmails verstuurd naar leerlingen vanuit mijn adres."*
>
> Collega Bert in *'De eerste Lijn'* nr. 23 (Klasse)

> *"Soms ben ik de school kotsbeu en dan is het tof om de leerkrachten belachelijk te maken. Soms neem ik stiekem een foto in de klas en dan bewerk ik die met een paar vrienden. Of we plukken foto's van de schoolsite, die van onze trip naar Parijs bijvoorbeeld. We sturen die dan door via gsm of op het internet."*
>
> Erike (17) in *'De eerste Lijn'* nr. 23 (Klasse)

Verschillen met gewoon pesten

Bij cyberpesten is het minder belangrijk dat het slachtoffer steeds weer opnieuw lastig gevallen wordt om van pesten te kunnen spreken. Een website met beledigende commentaar over iemand bijvoorbeeld, staat vaak voor een lange tijd en voor iedereen online. Een compromitterende foto of filmpje kan jaren later plots weer opduiken. Een gesproken belediging verdwijnt op het moment dat ze wordt uitgesproken.

Bij klassiek pesten is de fysieke kracht van de pester dikwijls belangrijk omdat die hem machtiger maakt dan zijn slachtoffer. Een cyberpester put vooral macht uit computer- en internetkennis.

Boodschappen via internet of gsm bevatten weinig tekens om de boodschap te interpreteren. We kunnen de gelaatsuitdrukking niet zien, de intonatie niet horen. Cyberpesters zien niet hoe hun slachtoffers reageren op de pesterijen, en beseffen zo nog minder hoe kwetsend hun boodschappen overkomen.

Op internet en met een mobieltje kan een jongere gemakkelijk een andere identiteit aannemen en anderen 'anoniem' lastigvallen in cyberspace.

Cyberpesten kan veel vormen aannemen

(1) Het wachtwoord van iemands e-mailadres ontfutselen, in zijn account inbreken en het wachtwoord veranderen zodat de betrokkene geen toegang meer heeft tot zijn persoonlijke post. Grafiek #1

(2) Inbreken in een computer en persoonlijke informatie stelen. Grafiek #3

(3) Enorm veel of grote berichten naar iemand sturen om zijn of haar computer te laten vastlopen. Grafiek #4

(4) Iemand beledigen of bedreigen via internet of gsm. Grafiek #5

(5) Compromitterende foto's of (webcam)filmpjes verspreiden via internet of gsm of ze op een website publiceren. Gemanipuleerde foto's verspreiden.

(6) Inbreken in de e-mail of messenger van een ander en van daaruit beledigende of compromitterende berichten sturen naar de contactpersonen uit het adresboek. Die krijgen dan de indruk dat de gepeste dat bericht zelf naar hen stuurde. Grafiek #9

(7) Op een website een kwetsende stemming houden over iemand (bv: Vind je Joris ook oerdom?). Grafiek #10

(8) Vertrouwelijke informatie op een website plaatsen of doorsturen naar anderen via sms of e-mail. Grafiek #11

(9) Vernederende informatie ('iedereen haat je') posten op weblogs. Grafiek #7

(10) Roddels verspreiden via internet of gsm. Grafiek #12

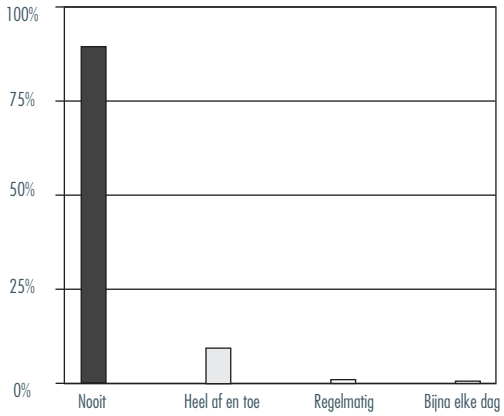
Dit lijstje toont aan dat het arsenaal van een cyberpester heel veelzijdig is. Tegenover de gewone pester beschikt hij over veel meer wapens. Alleen het fysiek intimideren ontbreekt in de cyberpestwereld. Dat sluit natuurlijk niet uit dat het cyberpesten soms een fysiek verlengstuk krijgt.

Gradaties

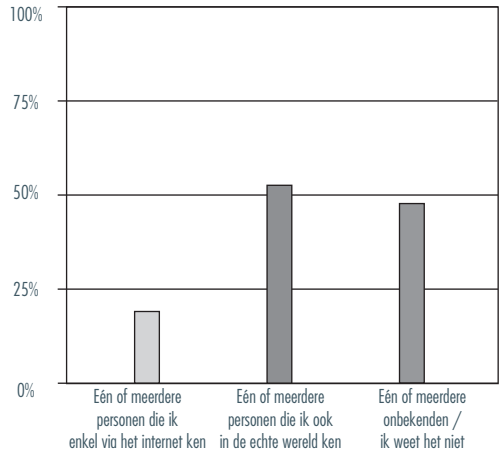
Als je die opsomming leest, merk je ook dat het gaat van 'plagen zonder grenzen' tot echt strafbaar gedrag. Wie een naaktfoto van een jongere rondstuurt of online publiceert, stelt zich bloot aan vervolging, want hij overtreedt de wet op de bescherming van de persoonlijke levenssfeer. Wie inbreekt in een persoonlijke mailbox, schendt de wet op het briefgeheim.

Het is belangrijk dat leraren jongeren daarop wijzen. Want zelf beseffen ze meestal niet hoe grensoverschrijdend hun gedrag is. Dat kan klassikaal als er zich een incident heeft voorgedaan. Merk je gewoon dat een individuele leerling te ver gaat? Spreek hem dan onmiddellijk persoonlijk daarover aan.

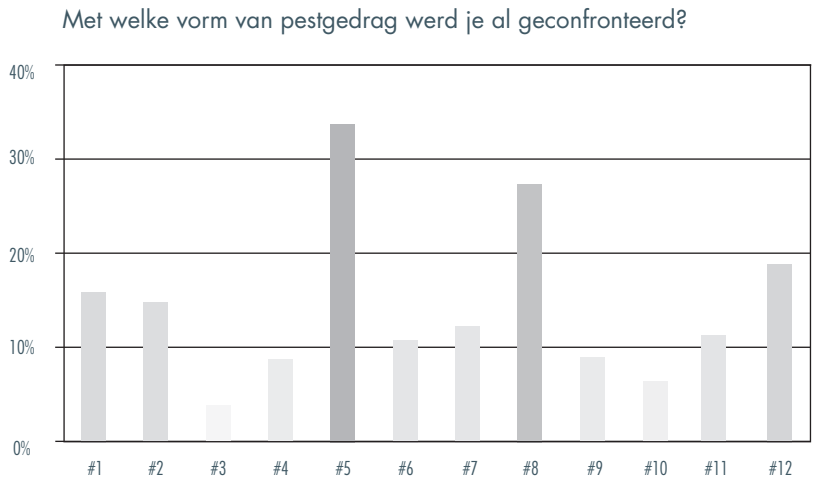
Het viWTA-onderzoek vroeg hoe vaak jongeren werden gepest tijdens de drie maanden voor het invullen van de vragenlijst.



Bron: Vandebosch, Heidi, Van Cleemput, Katrien, Mortelmans, Dimitri, Walrave, Michel, *Cyberpesten bij jongeren in Vlaanderen, studie in opdracht van het viWTA*, Brussel, 2006



Bron: Vandebosch, Heidi, Van Cleemput, Katrien, Mortelmans, Dimitri, Walrave, Michel, *Cyberpesten bij jongeren in Vlaanderen, studie in opdracht van het viWTA*, Brussel, 2006



#1 In jouw email inbox of Messenger ingebroken en het paswoord veranderd
#2 Opzettelijk een virus doorgestuurd
#3 Ingebroken in je computer en persoonlijke informatie gestolen
#4 Enorm veel of grote berichten naar jou gestuurd om je computer te laten vastlopen
#5 Jou beledigd of bedreigd via internet of GSM
#6 Jou uitgesloten uit een online groep
#7 Private of beschamende dingen over jou verspreid via internet of GSM
#8 Jou misleid door te doen alsof hij/zij iemand anders was
#9 Ingebroken in je e-mail of messenger en berichten gestuurd naar je contactpersonen
#10 Op een website een stemming gehouden waarbij gesteld werd dat jij niet leuk/mooi bent
#11 Dingen die iemand in vertrouwen had verteld, op een website geplaatst of doorgestuurd naar anderen via SMS of e-mail
#12 Roddels verspreid over jou via internet of GSM

Bron: Vandebosch, Heidi, Van Cleemput, Katrien, Mortelmans, Dimitri, Walrave, Michel, *Cyberpesten bij jongeren in Vlaanderen, studie in opdracht van het viWTA*, Brussel, 2006

uit BenX

Uit het viwta-onderzoek (zie grafiek) blijkt verder dat meer dan de helft van de pesters hun slachtoffer ook in het echte leven kennen. Maar 1 op 5 ontmoet hun slachtoffer alleen in cyberspace. In die gevallen is pesten dus een puur virtueel gegeven, dat wel keihard ingrijpt op het leven van het slachtoffer.

5.2 Preventieve aanpak

Scholen zonder pestbeleid zijn in Vlaanderen de uitzondering. Het komt er dus op aan cyberpesten te integreren in de globale aanpak van pesten.

Dat betekent in de eerste plaats een preventieve aanpak. De beste preventie is de zorg voor een positief schoolklimaat. Verder moeten leraren jongeren bewust maken dat:

(1) cyberpesten verregaande gevolgen heeft voor de slachtoffers: ze treffen een persoon met gevoelens, die zich zwaar gekwetst kan voelen door de manier waarop leeftijdgenoten met hen omgaan op internet of via gsm;

(2) risicogedrag op internet pesters meer kansen biedt (zoals doorgeven van wachtwoorden aan vrienden of doorgeven van persoonlijke informatie zoals naam, namen van familieleden of vrienden, adressen, telefoonnummers en kredietkaartgegevens op het internet plaatsen, foto's doorsturen…);

(3) pesterijen op het internet kunnen worden opgespoord en bestraft. Mogelijke sancties moeten eveneens duidelijk zijn.

De basisregel moet zijn: onze school tolereert geen pestgedrag.

Een goed uitgebouwd pestbeleid betekent ook dat de leerlingen weten bij wie ze terecht kunnen als ze het slachtoffer worden van pestgedrag of als ze pestgedrag bij anderen merken (zowel bij daders als bij slachtoffers). Daarbij is het belangrijk dat ze garanties krijgen over hun anonimiteit.

Meestal willen ze ook wel de zekerheid dat de pesters niet meteen worden bestraft. De drempel om wangedrag te melden, is veel groter als ze weten dat er voor de daders sancties aan vasthangen. Er is niet alleen de solidariteit voor de bestrafte pester, er is ook de vrees dat die wel eens wraak op hen zou kunnen nemen.

Betrek ook ouders uitdrukkelijk in de communicatie rond pestgedrag. Dan weten zij ook met wie ze contact kunnen opnemen als ze merken dat hun kind pest of wordt gepest. De meest aangewezen methode is een duidelijke samenvatting van het pestbeleid in de schoolbrochure die de ouders bij de aanvang van het schooljaar krijgen. Opname van maatregelen en eventuele sancties in het reglement voorkomt meteen discussies achteraf.

Vlaanderen telt heel wat organisaties die scholen helpen om een sluitend beleid tegen pesten uit te werken. Je vindt een overzicht op de website: www.kieskleurtegenpesten.be

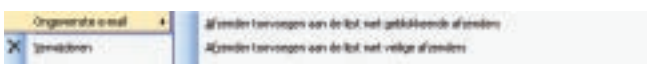
5.3 Curatieve aanpak

De jongeren die slachtoffer zijn van echt pestgedrag kunnen zelf, samen met hun leraar of ouders een aantal maatregelen nemen om pestgedrag een halt toe te roepen. De basisregel daarbij moet zijn dat je de klachten ernstig neemt en het slachtoffer steunt. Opvoeders moeten het slachtoffer steeds duidelijk maken dat het niet zijn schuld is dat hij wordt gepest en dat er geen reden is om zich schuldig te voelen.

Wat kan de leerling zelf doen?

(1) Als een leerling eens één keer een hatelijk bericht krijgt, kan hij dat best gewoon verwijderen en negeren. Een boos of gekwetst antwoord sturen is vaak de slechtste reactie, want dan puurt de pester voldoening uit de zekerheid dat hij raak trof.

(2) De meest laagdrempelige ingreep is het blokkeren van ongewenste e-mail. Een aantal gratis webmailaccounts biedt dit soort bescherming niet. De betere (b.v. hotmail en g-mail) doen dat wel. Als een jongere mailt met Outlook (Express) kan hij heel eenvoudig het e-mailbericht aanklikken met de rechtermuisknop en onder het item 'Ongewenste e-mail' de optie kiezen: 'Afzender toevoegen aan de lijst met geblokkeerde afzenders'.



Dit beschermt natuurlijk niet tegen de handige pester die doorheeft dat zijn berichten worden afgeblokt en een ander (gratis) e-mailadres kiest om pestberichten te blijven sturen.

(3) Een jongere die in een chatroom wordt gepest, kan een nieuwe nickname kiezen. Als hij verder geen contact heeft met de betrokkene, kan de pester die niet zo gauw achterhalen.

(4) Het slachtoffer kan ook een nieuw gratis e-mailadres kiezen. In die context is het belangrijk dat je jongeren leert dat ze best met minstens twee e-mailadressen werken. Eentje voor de echte vrienden waarbij ze heel goed opletten aan wie ze dit doorgeven. Een tweede voor een ruimere kring contacten. Worden ze op één adres gepest? Dan kunnen ze dat afsluiten. Met de echte vrienden kunnen ze zonder probleem blijven mailen.

(5) Sommige chatrooms hebben moderatoren die op vraag van de gebruikers ingrijpen bij ongewenst gedrag, dus ook bij pesterijen. Doet dit gedrag zich in dit soort chatroom voor? Dan spreekt de gepeste jongere best meteen de operator of moderator aan. Die kan de pester voor korte of langere tijd blokkeren. Dat ervaren pesters meestal als lik op stuk. Want nu zijn ze plots zelf de dupe van hun gedrag. Indien het om een privé chatruimte gaat is het moeilijker. Die wordt niet gemodereerd en daar doen de meeste problemen zich voor.

(6) Wordt een jongere gepest op een website? Dan kunnen ze best meteen de provider van de webruimte aanspreken. Die zal contact opnemen met de betrokkenen. Stopt de pester niet? Dan kan de provider de webruimte offline zetten.

Wat kan de de ICT-coördinator doen?

Binnen een elektronische leeromgeving kan de ICT-coördinator veel onheil voorkomen als hij het leerlingen onmogelijk maakt om berichten naar iedereen te versturen (zie hoofdstuk voor ICT-coördinatoren). Een haatbericht, een beledigende e-mail, een compromitterende foto die een pester via het schoolnetwerk rondstuurt, is vaak heel kwetsend. Want het slachtoffer staat voor aap voor de hele schoolgemeenschap. In een elektronische leeromgeving kan eventueel ook de forumfunctie uitge-

schakeld worden. Als die functie niet gebruikt wordt door de leraars is dit een aan te raden optie.

Wat kan je als leraar doen?

Wordt een leerling in je klas gecyberpest? Praat er dan in elk geval over in de klas en neem de klachten ernstig. Is de pester een klasgenoot? Dan kan een gesprek ertoe leiden dat hij eerlijk opbiecht. Dan stopt het pestgedrag ook meteen. Doet hij dat niet? Dan kan een gesprek vaak ook voldoende zijn om tips te krijgen van andere leerlingen die iets vermoeden en uit begrip voor het slachtoffer mee een einde aan de situatie proberen te stellen.

Sanctioneren van pesters

Vaak ervaren jongeren ook reacties en handelingen van anderen als pestgedrag, terwijl ze vinden dat ze zelf hun leeftijdsgenoten alleen maar wat 'plagen' als ze precies hetzelfde doen. Het is dus belangrijk gradaties in pestgedrag te onderscheiden en pas over te gaan tot sancties als er echt een grens is overschreden.

De meeste jongeren zien na een stevig gesprek met de leraar (of de directie) in dat er toch wel wat mis is met hun gedrag en stoppen ermee. Jongeren durven ook al wel eens iets stelen in een grote winkel. Na een flinke berisping op het bureau van de veiligheidsagent of directeur stopt dat ook meestal.

Heel wat scholen werken bij de aanpak van pestgedrag op school met de 'no blame'-aanpak. Deze methode vertrekt van een aanpak die niemand met de vinger wijst, maar alle betrokkenen samenbrengt: slachtoffers en daders, maar ook helpers en toeschouwers. Samen bespreken ze de situatie. Ze zoeken een oplossing waarbij iedereen erop toeziet dat het pestgedrag stopt en het slachtoffer ondersteuning krijgt van klasgenoten.

Bij cyberpesten is die aanpak vaak veel moeilijker, precies omdat pestgedrag zich daar vaak in een 'anonieme' één-éénrelatie tussen pester en slachtoffer afspeelt.

Sancties hebben vaak ook een voorbeeldfunctie. Misbruikte een leerling het schoolnetwerk of de elektronische leeromgeving voor pestberichten? Dan is het belangrijk dat de school met een sanctie duidelijk maakt dat ze dit soort gedrag niet duldt.

Politie inschakelen

Blijft het pestgedrag lange tijd duren en escaleert het? Lukt het niet om te achterhalen wie de dader is? Bijvoorbeeld omdat hij steeds van e-mailadres verandert? Gaat het pesten zo ver dat er inbreuken zijn op de wetgeving (bijvoorbeeld foto's rondsturen — zie hieronder: strafbaar gedrag)? Dan kun de hulp ingeroepen worden van de federale politie. Die heeft afspraken met de providers in Vlaanderen om de eigenaar van een IP-adres op te sporen.

In principe schakelt een school nooit de politie in als niet eerst contact is opgenomen met de leerlingenbegeleiding op school en het CLB. Het is ook niet aangewezen dat de school contact opneemt met de politie zonder de ouders van het slachtoffer hierover in te lichten. Want als er een officiële klacht komt, wordt ook het slachtoffer daarbij betrokken.

Ook de politie werkt overigens met gradaties. In eerste instantie zal de dader ook hier meestal alleen een waarschuwing krijgen. Er wordt een proces-verbaal opgesteld dat pas bezwarend wordt als het pestgedrag voortduurt of als dezelfde pester later een ander slachtoffer het leven zuur maakt.

Wat is strafbaar gedrag?

(1) inbreuken op de wet op de bescherming van de persoonlijke levenssfeer, zoals het verspreiden van (compromitterende) foto's;

(2) bedreigingen met fysiek geweld als het slachtoffer weigert iets te doen — zoals 'Als je me nu je wachtwoord niet geeft, dan krijg je morgen slaag';

(3) belaging (dat is de officiële term in de wet voor 'stalking'): het blijven verzenden van haatmail, dag en nacht sms-berichten versturen of telefoneren. Daarbij houdt de rechtspraak rekening met leeftijd en persoonlijkheid van het slachtoffer.

(4) inbreuken op de wet op de informatiecriminaliteit, zoals producten via internet bestellen op naam van het slachtoffer, hacking (inbreken in mail, website, profiel,…).

De politie grijpt alleen in als het pestgedrag herhaaldelijk is voorgekomen. En er is een formele kracht nodig.

Hoe bewijsmateriaal verzamelen?

Dat hangt af van het medium dat de pester gebruikt. Bewaar bij pesterijen

via e-mail:

- **(1)** e-mailadres;
- **(2)** uur en datum van ontvangst;
- **(3)** kopies van de e-mails inclusief de volledige kopteksten (headers).

in online vriendengroepen

- **(1)** websiteadres (URL) van de MSN-groep die pestgedrag vertoont;
- **(2)** schuilnaam (nickname) en e-mailadres van de pester;
- **(3)** datum waarop het pestgedrag zich voordeed.

via profielsites

- **(1)** websiteadres (URL) van het profiel;
- **(2)** schuilnaam (nickname) en e-mailadres van de pester;
- **(3)** datum waarop je het pestgedrag opmerkte.

in chatrooms

- **(1)** datum en uur waarop werd gechat;
- **(2)** naam en websiteadres (URL) van de chatroom);
- **(3)** schuilnaam (nickname) en e-mailadres van de pester;
- **(4)** schermafdruk van de chatroom met kwetsende commentaren.

5.4 Meer informatie

Websites

De Eerste Lijn over cyberpesten van Klasse:
klasse.be/kvl/163/49: op cd-rom bij dit boek
www.pesten.net
www.cyberpesten.be

Tips voor kinderen basisschool: www.yeti.be
— links onderaan op de rode knop drukken.

Boek: *'Pesten is Laf. Cyberpesten is nog laffer!'*,
met website: www.pestenislaf.nl.

Lectuur en lespakketten

Lesmateriaal over cyberpesten voor het lager onderwijs en het secundair onderwijs op de cd-rom bij deze publicatie
Lespakket van Sensoa, eveneens op de cd-rom
Onderzoek van UA in opdracht van ViWTA: www.viwta.be
— publicaties – rapporten: je kunt de samenvatting en het volledig verslag downloaden.

Organisaties

Links naar organisaties die scholen ondersteunen bij het uitwerken van een beleid tegen pesten vind je op:
www.kieskleurtegenpesten.be/

.6.

RESPECT VOOR INTELLECTUELE EIGENDOM

Auteursrecht is uitgesteld loon. Een auteur — schrijver, tekenaar, fotograaf, softwareontwikkelaar,… — verwerft geen inkomsten tijdens zijn 'arbeidsproces', maar wel op het ogenblik dat zijn werk in de openbaarheid komt: als een liedje op de radio wordt gedraaid, een tekst wordt gedrukt, een foto in de krant verschijnt, een filmfragment wordt vertoond, een softwarepakket draait op een pc.

De artistieke of intellectuele verdiensten van het werk zijn niet van belang: ook doordeweekse tekeningen of foto's komen in aanmerking voor bescherming. De enige voorwaarde is dat het werk de uiting is van de persoonlijkheid van de auteur. Een zuivere kopie of een elementaire samenvatting (waarbij er geen sprake is van eigen creatieve inbreng) worden dus niet auteursrechtelijk beschermd. De herinterpretatie van een bestaand werk kan echter wel in aanmerking komen.

Kenmerken

Auteursrechten zijn geen belasting, maar een recht dat 'werken van de geest' beschermt. SABAM, de Belgische vereniging voor auteursrechten vermeldt een aantal kenmerken.

(1) Auteursrecht ontstaat bij de schepping van het werk. Het vergt geen enkele formaliteit of voorafgaande deponering.

(2) Nieuwheid is geen vereiste, maar het werk moet een origineel karakter hebben en de stempel van de maker dragen.

(3) Het werk moet in een vorm gegoten zijn, een louter idee is niet auteursrechtelijk beschermd.

(4) De beschermingstermijn bedraagt 70 jaar na het overlijden van de auteur. Deze termijn blijft gelden ook als het werk niet wordt gebruikt.

zie: www.sabam.be

Basisprincipe

Het basisprincipe is dat je alleen reproducties mag maken mits toestemming van de auteur.

De auteurswet bevat echter twee belangrijke uitzonderingen: je mag een kopie maken voor strikt privégebruik en je mag reproducties maken voor onderwijs of wetenschappelijk onderzoek. Dat laatste gebeurt wel met een belangrijke beperking: het gebruik moet vallen binnen de niet-winstgevende doelstelling van de school en de reproductie mag geen afbreuk doen aan de 'normale exploitatie van het werk'. Ook de Europese wetgever erkent de inperking van het absolute recht van de auteur voor onderwijs, onderzoek en cultuur.

Je mag dus in de klas kopies ronddelen of tonen van de denker van Rodin, een gedicht van Herman de Coninck, een fragment uit Kartonnen Dozen van Tom Lanoye. Maar je mag niet de volledige dichtbundel of roman gekopieerd uitdelen. Binnen de wet op het reprografierecht betaalt de school hiervoor een vergoeding via de belasting op fotokopies. De fragmenten publiceren op een schoolwebsite mag enkel als daarvoor toestemming is verkregen of auteursrechten zijn betaald.

Zoekmachines

Veel leraren denken: 'Welke auteur vindt nu die reproductie op onze website?'. Houd er dan wel rekening mee dat er zoekmachines zijn (en niet alleen de publieke zoals Google en Yahoo, maar ook zeer specifieke) die het web afspeuren op illegale kopies. Een aantal scholen kreeg al een veroordeling omdat ze beschermd werk op hun website publiceerden zonder de nodige rechten te betalen.

Betaal je een fotograaf om foto's te nemen van een schoolactiviteit? Teken dan een contract waarin de school de copyrightrechten verwerft. Anders behoudt de fotograaf het auteursrecht en kan hij achteraf een extra vergoeding eisen.

6.1 Wat valt onder auteursrecht?

Teksten

Teksten zijn enkel 100 procent veilig als je zelf de auteur bent. Het kopiëren van een bestaande tekst impliceert uiteraard niet dat je zelf de auteur van de tekst wordt. Het doet er niet toe hoe lang hij is — een slogan, enkele regels of verschillende pagina's. Wanneer je iets overneemt, doe dat dan als een citaat en vergeet niet de bron te vermelden. Het doet er ook niet toe of op welke informatiedrager de tekst aanvankelijk geplaatst werd.

Foto's

Als je zomaar een foto downloadt, kopieert of inscant loop je steeds het risico dat je een copyright schendt. Bij foto's schuilt er nog een extra addertje onder het gras. Je hebt niet enkel de toestemming van de auteur nodig maar in sommige gevallen moet je ook de toestemming krijgen van de auteur van het gefotografeerde voorwerp of van de persoon op de foto. Zie ook hoofdstuk 3.4 Foto's op de schoolwebsite.

Monumenten

Wees ook voorzichtig met voorbereidingen of verslagen van studiereizen die je als leraar online zet. Heel wat monumenten

of beeldhouwwerken in het straatbeeld vallen onder de wet op het auteursrecht. Een voorbeeld in eigen land is het Atomium. Als je een foto van dat gebouw op je website plaatst, moet je auteursrechten betalen aan SABAM.

Reproducties van kunstwerken

Let op met de interpretatie van de regel dat het auteursrecht vervalt als de kunstenaar meer dan 70 jaar overleden is. Als je ergens een knappe foto vindt van de Mona Lisa, betekent dat niet dat je die zomaar mag publiceren. Want voor een foto geldt het auteursrecht van de fotograaf die de foto maakte. En die is misschien geen 70 jaar overleden. Soms beheert het museum waar het werk werd tentoongesteld zelf de auteursrechten.

Nam je zelf in een museum een foto van een kunstwerk waarvan de maker meer dan 70 jaar geleden overleed? Dan zal een vereniging van auteursrechten zoals SABAM geen rechten kunnen opeisen. Maar misschien tikt het museum zelf je op de vingers. In musea geldt vaak een verbod op het nemen van foto's. Deed je dat toch en publiceer je die foto? Dan kan het museum je strafrechtelijk vervolgen voor illegale foto's.

Muziek en films

Leerlingen denken vaak dat muziek algemeen cultureel erfgoed is. En dat ze dus vrij mogen beschikken over muziekbestanden. Dat gaat zover dat ze er geen graten inzien om gekopieerde mp3-bestanden of cd's aan vrienden te verkopen. Hetzelfde geldt voor films.

Kazaa garandeert nu dat zijn software spywarevrij is. Ergens ver weg in de voorwaarden (en wie leest die?) staat: "Installation. When you install the Software, the install program (…) is saved to your My Shared Folder and shared out to other users. You understand and agree that other users may download this file from your computer and by doing so your Internet connection will be used." Met andere woorden: je pc wordt een zombie (zie hoofdstuk 5).

Het is daarom een belangrijke taak voor het onderwijs om leerlingen goed uit te leggen wanneer ze strafbare feiten plegen.

Niet-strafbaar:

(1) Je koopt een cd/dvd in de winkel en maakt een kopie voor eigen gebruik (bv. voor je walkman of op kot).

(2) Je downloadt muziek van je favoriete groepje dat op zijn website expliciet toestemming geeft om dat gratis te doen.

(3) Je downloadt muziek van een legale muzieksite van de platenfirma zelf of een website met licentierechten en je betaalt een vergoeding voor de nummers. Ook dan mag je een kopie maken op een drager voor persoonlijk gebruik.

Strafbaar:

(1) Je koopt een cd/dvd in de winkel, maakt kopies en verkoopt die.

(2) Je verspreidt zelf tegen betaling muziek die je met toestemming gratis downloadde van de website van een (lokale) muziekgroep.

(3) Je downloadt muziek van een illegale muzieksite. In dit geval is het downloaden op zich al strafbaar.

(4) Je downloadt muziek van een legale muzieksite, maakt kopies en verkoopt die.

Extra punt: wie downloadt van een illegale muzieksite, gaat meestal automatisch deel uitmaken van een peer-to-peer netwerk. Daarin halen de gebruikers de muziek van elkaars computers en maken ze zich meteen ook schuldig aan het verspreiden van illegale muziekbestanden.

Software

Als de school leerlingen probeert op te voeden tot eerlijkheid en respect voor rechtsnormen, moet ze zelf het voorbeeld geven. Gebruik geen illegale software en geef ze zeker iet door aan leerlingen, zoals je ook geen boeken kopieert en ronddeelt.

Illegale kopies hebben hoe dan ook grote nadelen. Je loopt als school altijd het risico op een boete van de BSA (Business Software Alliance). En nog belangrijker: je hebt geen recht op updates en patches (klein stukje software dat de uitgever van software gebruikt wordt om fouten aan zijn software te herstellen).

Gebruik je software uit het commerciële circuit? Zorg dan dat de school voldoende officiële licenties aankoopt. Dat kan meestal tegen 'academische prijzen'. Die liggen een stuk lager dan de prijzen die bedrijven of particulieren betalen. Een voorbeeld zijn de Microsoft-licenties binnen de MS-KIS overeenkomst die dat bedrijf met de Vlaamse overheid afsloot. Maar er zijn ook heel wat andere bedrijven die op hun website of via hun dealers speciale tarieven hanteren voor het onderwijs. IBM stelt een aantal softwareprogramma's gratis ter beschikking van scholen. Achteraan dit hoofdstuk lees je hoe je deze cd-rom en de IBM-software kunt bestellen.

Voor een school die geen geld wil uitgeven aan software en toch ethisch wil handelen, bestaat er een alternatief: vrije software. Bij vrije software stellen de ontwerpers de broncode vrij ter beschikking. Ze gebruiken hun auteursrechterlijke bescherming om aan die broncode een licentie te koppelen die vrij gebruik toelaat. Men mag de software kosteloos en zonder expliciete toelating op een onbeperkt aantal computers gebruiken, aanpassen, verspreiden en integreren met andere software. Eventuele beperkingen (zoals verkoop) worden beschreven in de licentie die bij de software hoort. Elke school en ICT-coördinator ontving in 2006 van de Vlaamse overheid de cd-rom *"Vrije software in het onderwijs"*. De cd bevat een selectie van softwaretoepassingen voor een educatieve context.

Op de cd-rom bij deze publicatie vind je een handleiding voor softwarebeheer van de BSA. Deze handleiding is vooral nuttig voor ICT-coördinatoren en kan gebruikt worden om zowel de commerciële als vrije software op school te beheren.

6.2 Auteursrecht en schoolnetwerken

Steeds meer scholen werken met een elektronische leeromgeving. Dat is in feite een vorm van intranet, een afgeschermde omgeving waar de buitenwereld geen toegang toe heeft. Het is alleen toegankelijk voor leraren en leerlingen met een gebruikersnaam en wachtwoord. Leraren en leerlingen gebruiken het als hulpmiddel bij lessen, om opdrachten uit te wisselen, enz. De school kan het ook gebruiken voor algemene mededelingen, een nieuwsbrief, enz.

Een elektronische leeromgeving is dus een afgeschermde internet- of netwerkomgeving. Als je een foto van een kunstwerk binnen de elektronische leeromgeving publiceert om daarmee het lesonderwerp te illustreren, gaat het om lesmateriaal. Dat is een strikte onderwijsaangelegenheid, zoals je een reproductie op papier afdrukt om je les te illustreren. Dat is niet verboden.

De zaken liggen natuurlijk anders wanneer je datzelfde kunstwerk publiceert op de website van de school. Want iedereen kan via een zoekmachine of toevallig naar je webpagina surfen en daar je reproductie van het beschermde kunstwerk vinden. Publicatie op een website kun je niet klasseren onder 'privégebruik' en valt ook niet onder de soepeler norm 'onderwijs'.

Wat mag?

Wat mag een school op haar website of elektronische leeromgeving zetten? Mag een leraar een cursus in de elektronische leeromgeving of op de website plaatsen met reproducties van kunstwerken? Of een fragment uit een roman? Mag je tekeningen van kleuters zomaar online publiceren? Wat als leerlingen via het schoolnetwerk muziek downloaden?

Hyperlinken
Gewone hyperlink

In principe mag je vrij hyperlinks leggen naar andere websites. Je kopieert immers niets, maar verwijst de gebruiker door naar mogelijk interessante informatie. Gaat het om een heel specifieke website? Twijfel je of de auteur een link wel zal appreciëren? Neem dan even contact op met de beheerder van de webpagina's en vraag zijn akkoord. Soms heb je zelfs een website die uitdrukkelijk vermeldt dat je alleen een hyperlink mag leggen als je de expliciete toestemming hebt van de eigenaar.

Deeplinken

Dat doe je in elk geval best wanneer je werkt met 'deeplinking': je legt een hyperlink naar een specifieke pagina op de website. Zeker als op die pagina geen vermelding staat van de eigenaar van de website, is het aangewezen dat je toestemming vraagt of in elk geval bij je hyperlink vermeldt naar welke website je de bezoeker stuurt. Een nadeel van deeplinken is ook dat je het risico loopt dat de bewuste pagina verdwijnt of van naam verandert.

Geframede link

Leg je een hyperlink? Open die andere website dan altijd in een nieuw venster en trek de andere website niet 'in de jouwe' via de framing-techniek. Dan kun je onterecht de indruk wekken dat die pagina deel uitmaakt van jouw website.

Betrouwbaarheid gegarandeerd?

Als webmaster ben je verantwoordelijk voor de hyperlinks die je legt. En dus is er een 'maar' bij links. Ook al heb je vandaag goed nagedacht over de adressen waarnaar je verwijst, heb je geen garantie over wat er morgen of later met de inhoud gebeurt.

Leerlingensites

Als school moet je ook opletten voor webpagina's die je leerlingen laat maken. Als je die laat publiceren onder de domeinnaam van de school, dan is de school verantwoordelijk voor wat erop staat. Dat geldt ook als je werkjes van leerlingen online zet opdat de ouders ze kunnen inkijken. Zorg dan dat de leerlingen alle regels naleven.

> *"De websites die leerlingen maken, staan niet onder de domeinnaam van de school. Ze mogen best zelf websites ontwerpen, maar dat is dan onder hun eigen verantwoordelijkheid. Wat betreft het auteursrecht is onze school alleen aansprakelijk voor haar eigen pagina's."*
>
> Herman Vansteenkiste, directeur van het Handelsonderwijs Burgerschool in Roeselare.

Het zelfde geldt voor weblogs van individuele leerlingen en klassen. De auteur is verantwoordelijk. Staan die blogs op de schoolwebsite? Dan moet de webmaster ze opvolgen. Dat geldt ook voor (webcam)filmpjes die ze op de website plaatsen.

6.3 Tips

Tip 1: Vraag toestemming

Er is de slimme weg. Veel auteurs en organisaties zijn heel welwillend tegenover onderwijs. Vraag gewoon of je een foto, reproductie of citaat uit een werk mag publiceren op je website. Heel vaak krijg je het positieve antwoord: 'Doe gerust. En… het mag gratis.' Of je betaalt slechts een fractie van de normale rechten. Daarbij is het wel van belang dat je duidelijk maakt dat de overname een strikt didactische bedoeling heeft en niet als doel heeft om je website op te fleuren.

Tip 2: Zorg voor correcte bronvermelding

Als je teksten van anderen gebruikt op een website, moet je altijd zorgen voor een correcte bronvermelding. Er zijn trouwens nogal wat websites van de overheid of culturele organisaties die uitdrukkelijk vermelden dat je er kosteloos mag uit citeren op voorwaarde dat je de bron vermeldt. Teksten uit deze publicatie mag je bijvoorbeeld altijd gratis citeren met vermelding van de bron: het Vlaamse Ministerie van Onderwijs en Vorming.

Bronvermelding is ook nodig als je teksten parafraseert. Of als je foto's bewerkt met een beeldverwerkingsprogramma. Houd daarbij ook rekening met de regel dat een aanpassing of vervorming van een auteursrechtelijk beschermd werk inbreuk kan doen op het morele 'recht op integriteit van het werk'. En dan is de toestemming van de auteur vereist.

Tip 3: Vrij van auteursrecht?

Op het internet vind je databanken met werken (foto's, beelden of software) waarbij vermeld staat dat de werken 'zonder auteursrechten' zijn en dat je ze vrij mag reproduceren (zie enkele website-adressen aan het einde van dit hoofdstuk). Het

feit dat de houders van de rechten verklaren dat het werk 'vrij van rechten' is, klopt niet helemaal, want het auteursrecht blijft altijd van kracht. Je kunt wel stellen dat de houders een gratis gebruiksvergunning toekennen.

In zo'n geval moet je op twee zaken letten. Ten eerste staan bij het gebruik soms beperkingen, bijvoorbeeld dat het gebruik voor commerciële doeleinden uitgesloten is. Ten tweede is het mogelijk dat de vermeende houder van de rechten niet de echte houder is van die rechten. In dat geval kan de auteur zich later bekend maken en zich verzetten tegen het gebruik van zijn werk. Daartegen heb je als gebruiker geen verhaal.

6.4 Rechten op eigen werk

Natuurlijk heb je als leraar ook zelf auteursrecht op de teksten en kunstwerken die je zelf thuis creëert en zelfs op die, die je in opdracht van de school maakt. De school (inrichtende macht) heeft wel het auteursrecht op softwarematerialaal dat binnen de schoolmuren of in opdracht van de school tot stand komt. In alle andere gevallen behouden leraren zelf het auteursrecht, tenzij die uitdrukkelijk anders wordt overeengekomen, bv. in de arbeidsovereenkomst.

Dat recht verwerf je automatisch. Je hoeft er geen stappen voor te zetten. Toch is het aangewezen de tekst 'Copyright [naam van de school, leraar of leerling]' te vermelden onderaan elke pagina van de school, en zeker op alle didactisch materiaal.

Mogen andere scholen wel vrij gebruik maken van dat materiaal?
Voeg er dan aan toe: "Dit document mag enkel gekopieerd en gewijzigd worden voor niet-commerciële educatieve doeleinden en enkel met opname van deze verklaring. Reproductie, wijziging en verdeling van dit document is niet toegelaten zonder de instemming van de auteur."

De 'Creative Commons' licentie biedt een kader om de beperking 'Alle rechten voorbehouden' te wijzigen tot 'Sommige rechten voorbehouden'. Je bepaalt zelf wie onder welke voorwaarden (b.v. duidelijke bronvermelding, uitsluitend voor onderwijsdoeleinden) jouw materiaal mag gebruiken. Meer informatie op www.creativecommons.org.

6.5 Plagiaat tegengaan

Het wereldwijde web en digitale encyclopedieën zitten boordevol documentatie. Het is belangrijk dat leerlingen die van jongs af leren verkennen en zinvol gebruiken. Daarbij is het een taak voor de leraar om ze meteen te leren dat ze respect moeten opbrengen voor de intellectuele eigendom van anderen. Je aanvaardt niet dat ze hun taak overschrijven van hun buur of beste vriend. Aanvaard ook niet dat ze klakkeloos knippen en plakken uit hun encyclopedie op cd-rom of van het internet.

Leer correct citeren

De beste aanpak is de positieve: moedig leerlingen aan om bronnen te raadplegen én te citeren. Dat stimuleert ze om informatie te zoeken, te beoordelen en er gevatte uitspraken uit te lichten die in de context passen. Een vaardigheid die ze hun hele schoolcarrière lang nodig zullen hebben.

Zo kom je er als leraar meteen achter waar ze hun informatie halen. Dat kun je vervolgens bijsturen als je de indruk hebt dat je leerlingen eenzijdige of onbetrouwbare bronnen raadplegen. Je achterhaalt ook vlugger of ze meer dan alleen die enkele citaten hebben geknipt en geplakt. Leerlingen bieden je zo op een blaadje ideaal materiaal om toe te lichten hoe ze ethisch én kritisch kunnen omgaan met bronnenmateriaal.

Wees creatief met huiswerk en opdrachten

Het is een kwaal die onze leraren vroeger niet kenden. Er waren hoogstens wat boekbesprekingen die jongeren van oudere broer of zus, of van een leerling uit een hogere klas overschreven. Vaak waren die dan niet zo lang geleden voor dezelfde leraar geschreven en viel plagiaat meteen op.

Nu is er een keure huiswerksites met boekverslagen, spreekbeurten, vakgerichte dossiers, enz. Voor Vlaanderen is 'scholieren.pagina.be' een overzichtspagina waar je links vindt naar een heleboel websites. Nederland heeft 'huiswerk.nl'. Je kunt natuurlijk ook googlen naar: huiswerksites, boekverslag, recensie...

De beste methode tegen het huiswerkplagiaat bestaat in het maken van unieke, uitdagende opdrachten. Zorg voor doelgerichte opdrachten waarvoor ze de resultaten niet eenvoudig kunnen knippen en plakken. Er bestaat ook speciale, commerciële software die scholen helpen om plagiaat te bestrijden, zoals Ephorus en Urkund.

Leer herschrijven

Je kunt je leerlingen zelf op weg zetten met een oefening. Je zoekt zelf uit wat op diverse sites staat over één onderwerp. Dat geeft je meteen de kans om ze het verschil te leren zien tussen betrouwbare en onbetrouwbare informatie (zie hoofdstuk 2 over betrouwbare informatie). Je toont hoe ze daaruit, met toevoeging van eigen interpretatie en inzichten, een sluitend geheel maken. Je leert ze dan meteen welke zinnen geschikt zijn om letterlijk te citeren. Je vindt uitgewerkte voorbeelden op www.klascement.net (typ 'webquest' in als zoekterm en kies voor 'edudocs').

Laat leerlingen onderaan een lijst toevoegen van alle bronnen die ze raadpleegden. Dan heb je meteen een sterk wapen in de hand als ze hun tekst klakkeloos kopieerden van die ene website of encyclopedie die ze uit hun overzicht weggomden.

Geef het goede voorbeeld

Het spreekt voor zich dat leraars best zelf het goede voorbeeld geven en in hun cursussen correct verwijzen en citeren als ze materiaal van derden gebruiken. Een leraar die zelf plagieert of illegaal kopieert kan bezwaarlijk verwachten dat zijn of haar leerlingen wel de auteursrechten van anderen respecteren.

6.6 Meer informatie

Vrije software

Surf naar: www.ond.vlaanderen.be/ict/infrastructuur/ voor:

(1) Advies van de werkgroep onderwijs over vrije software: http://www.ond.vlaanderen.be/ict/infrastructuur/vrijesoftware/advies_vrije_software_werkgroep_onderwijs.pdf

(2) De brochure 'Vrije software in het onderwijs: een praktische gids voor het gebruik van open source software en open leermiddelen' http://www.ond.vlaanderen.be/ict/infrastructuur/vrijesoftware/vrije_software.pdf

Download vrije software op: vrijesoftware.klascement.net

Het grootste open software netwerk: sourceforge.net

Raamovereenkomsten

Surf naar: www.ond.vlaanderen.be/ict/infrastructuur/ voor:

(1) Infofiche over het softwareaanbod van IBM: http://www.ond.vlaanderen.be/ict/infrastructuur/IBMsoftwareaanbod.htm

(2) Educatieve korting op softwarelicenties, in uitvoering van de Microsoft Onderwijs KIS Overeenkomst: http://www.ond.vlaanderen.be/ict/infrastructuur/MSKIS05-NL.pdf

Academische licenties: www.signpost.be

http://www.gnu.org/

Handleiding voor gebruik vrije software van het Steunpunt voor Sociaal-Cultureel Volwassenenwerk: www.socius.be/handleiding/

Auteursrecht

www.sabam.be

www.internet-observatory.be rubriek juridisch kader – Intellectuele eigendom

www.mineco.fgov.be – zie onder intellectuele eigendom

www.bsa.org: de "Handleiding Softwarebeheer" vind je integraal op de bijgevoegde cd-rom

Collecties met open leermiddelen

Afbeeldingen: www.openclipart.org

Boeken: www.gutenberg.org

Partituren: www.mutopia.org

Foto's: www.sxc.hu

Huiswerksites

www.scholieren.pagina.be

www.huiswerk.nl

www.scholieren.com

www.huiswerk.leerlingen.com

www.collegenet.nl

www.verslagen.be

Bestrijd plagiaat:

www.ephorus.nl

www.urkund.com

.7.

BLIJF ER GEZOND BIJ

Hoewel de medische wereld nog geen sluitend antwoord kan bieden op de vraag naar de psychosociale en fysieke gevolgen van computergebruik in de samenleving, is enige realiteitszin wel vereist. Het is natuurlijk onzin dat de invoering van ICT op school de gezondheid van de Vlaamse jeugd ondermijnt. Fysieke risico's zijn enkel aan de orde als kinderen overdreven lang voor de computer zitten of als ze voortdurend in een verkeerde houding werken.

Overmatig en langdurig computergebruik of het aannemen van een foute houding aan de computer kan leiden tot RSI. RSI staat voor 'Repetitive Strain Injury', een verzamelnaam voor klachten in nek- en schoudergebied, armen, ellebogen, polsen, handen en vingers. Vaak hoor je ook de term 'muisarm' voor de typische pijn, stijfheid en tintelingen bij mensen die urenlang computeren. Meer dan de helft van de RSI-patiënten slikt dan ook regelmatig pijnstillers. Volgens een onderzoek van de European Foundation for the Living and Working Conditions heeft ongeveer 15% van de Belgische bevolking te kampen met RSI.

Gezien deze cijfers stellen scholen best het voorzorgsprincipe voorop om te vermijden dat de ontwikkeling van kinderen geremd wordt door (overmatig) computergebruik. De school kan met een preventief beleid de eventuele risico's uitschakelen. Veilig ICT-gebruik op school betekent investeren in een aangepaste infrastructuur en een gedoseerd en correct computergebruik. Het aanleren van goede attitudes in de computerklas heeft trouwens ook een positief effect op het gebruik van de computer thuis.

Gezond computeren doe je in vijf stappen:

- **(1)** koop het juiste materiaal;
- **(2)** richt de computerklas correct in;
- **(3)** beperk de duur van het computergebruik;
- **(4)** wijs op een goede houding;
- **(5)** wees alert voor RSI en verwijs eventueel door naar CLB of arts.

Daarbij is het de taak van ICT-coördinator om de juiste infrastructurele basisvoorwaarden te creëren.

7.1 Koop het juiste materiaal

Waar liggen de oorzaken van RSI? Vooral in onaangepast meubilair en een slechte houding. Daarom is het van belang dat scholen het goede voorbeeld geven met geschikt meubilair. Voor bureaus voldoen standaardoplossingen voor 95% van de leerlingen. De school moet alleen maatoplossingen voorzien voor de kleinste en grootste leerlingen. In de hoogte verstelbare stoelen in computerlokalen zijn wel een basisvereiste.

Bureau en bureaustoel

In een ideale situatie kun je zowel bureaublad als bureaustoel (zitvlak én rugleuning) in de hoogte verstellen. Het bureaublad heeft minimaal een diepte van 80 cm en een breedte van 120 cm — ideaal is een diepte van 100 cm. Het oppervlak heeft een matte en lichte kleur.

De armleuning van de stoel komt op gelijke hoogte met de werktafel. Pas bij voorkeur de bureauhoogte aan. Is dat niet mogelijk? Sleutel dan aan de stoelhoogte. Als je dan de voeten niet meer plat op de grond kunt zetten, gebruik je best een voetensteun. Stel de zitdiepte in zodat je een vuist kunt steken tussen de knieholte en de voorste rand van de zitting. Laat de stoel licht naar voren hellen, dat bevordert de natuurlijke kromming van de rug.

Een verrolbare bureaustoel heeft om veiligheidsredenen vijf wielarmen als bescherming tegen kantelen.

Schermtype

Een CRT-scherm (Cathode Ray Tube of kathodestraalbuis — de 'beeldbuis' van de klassieke televisie) stuurt een elektronenschaal naar een fluorescentiescherm om beelden te tonen. Dit schermtype is onderhevig aan flikkering omdat het beeld constant wordt 'ververst'. Stel de vernieuwingsfrequentie ervan in op minimum 70 Hertz. Slechtzienden die met vergrotingssoftware werken, mogen de frequentie niet instellen boven 80 Hertz.

Een lcd-scherm (Liquid Crystal Display of vloeibaar-kristalscherm) is een plat beeldscherm waarbij piepkleine transistors de beeldinformatie per pixel (puntje op het scherm) vasthouden. Dit type is minder belastend voor de ogen omdat het vrij is van vermoeiende flikkering.

Bron: Werken met beeldscherm op kantoor, FOD Werkgelegenheid, Arbeid en Sociaal Overleg

De vernieuwingsfrequentie van het beeldscherm wijzig je in Windows onder Configuratiescherm > Vormgeving en Thema's > Beeldscherm > Instellingen > Geavanceerd > Beeldscherm.

Computermuizen

Verkies een optische of lasermuis. Gebruik je toch een muis met een balletje? Reinig het dan regelmatig.

Een goede muis is niet te dik. Hoe dikker de muis, hoe meer de hand achterover buigt. Dat is erg belastend. Voor mensen met kleine handen is een polssteun een oplossing. Leg de muis dicht bij het lichaam en het toetsenbord. Houd ze in de hand in het verlengde van de onderarm, buig de pols niet achterover of naar links of rechts. Laat de zijkant van de handpalm op de muismat rusten. Leg de muis voor in de hand en laat de vingers ontspannen op de muisknoppen rusten (dus niet krampachtig erboven houden en niet knijpen).

De vernieuwingsfrequentie van het beeldscherm wijzig je in Windows onder Configuratiescherm > Vormgeving en Thema's > Beeldscherm > Instellingen > Geavanceerd > Beeldscherm.

Voor de kleuters kun je de aankoop overwegen van kindermuizen. Een gewone computermuis is te groot is voor kleine handjes. Daarom kunnen kinderen ze over het algemeen niet nauwkeurig bewegen. Een kindermuis is kleiner van formaat. Zo hebben kinderen een betere grip op de muis. Ook de knoppen zijn aangepast aan een kinderhand. Je vindt informatie op www.kindermuis.nl en www.kleutermuis.nl.

7.2 Richt de computerklas correct in

Beeldscherm

Een goed beeldscherm is draai- én kantelbaar. Zit recht voor het beeldscherm en plaats het 50 tot 70 cm van je ogen. De bovenzijde van het beeldscherm staat op ooghoogte. De kijkhoek is dan ongeveer 30 graden. Een grotere hoek kan nekklachten veroorzaken. Gebruik eventueel een monitorverhoging.

Verlichting

Ook de verlichting is belangrijk. Zorg in een computerklas voor zonwering en indirecte verlichting. Plaats de beeldschermen dwars op het raam zodat je reflectie vermijdt.

Muissnelheid

Zorg voor een goede instelling van de snelheid van muisbewegingen en dubbelklik. Als meerdere muisbewegingen (optillen en opnieuw plaatsen) nodig zijn om de cursor over het beeldscherm te bewegen, is de muis te langzaam ingesteld. Staat de muis echter te snel ingesteld, dan schiet de cursor zelfs met een kleine beweging al over het doel heen.

Moet je vaak lang aan een stuk gegevens overtypen van papier? Gebruik dan een documenthouder.

Test de dubbelkliksnelheid door op het mapje te dubbelklikken (Windows configuratiescherm > Printers en andere hardware > Muis)

Laptops

Werk je veel met een laptop? Plaats die dan op een verhoog. Als je een laptop gewoon op een tafel plaatst, is de lichamelijke belasting immers driemaal zo groot. Je kijkt dan in een te grote hoek naar beneden en riskeert nekklachten. Als je meer dan twee uur met een laptop werkt, moet je een apart toetsenbord en muis gebruiken.

Deze regels gelden ook voor scholen die leerlingen constant met een laptop laten werken in de klas.

7.3 Beperk de duur van het computergebruik

Vermijd om lang in eenzelfde houding te zitten. Ga regelmatig opnieuw goed zitten op je stoel, want ongemerkt zak je tijdens het werk lichtjes onderuit. Las regelmatig een korte pauze in en loop even rond. Lessen in de computerklas worden heel vaak gegeven in blokken van twee of meer aaneensluitende uren. Laat de leerlingen dan geen twee uren aan een stuk doorwerken, verplicht ze om tussen twee lesuren in even te bewegen. Zo leren ze een goede werkattitude.

Rode ogen

De meeste wetenschappers zijn het erover eens dat computergebruik slechts een lichte impact heeft op de ogen van kinderen. Jongeren ervaren dezelfde problemen als volwassenen als ze té lang naar een beeldscherm staren: prikkelende ogen, oogmoeheid, wazig gezichtsveld, hoofdpijn. De medische wereld vond voor de erge gevallen wel een specifiek woord uit: CVS of computervisiesyndroom.

Houd er wel rekening mee dat je bij het aantal uren achter het computerscherm het aantal uren tv-kijken optelt. Kinderen kunnen wel tegen een stootje, maar weten soms van geen ophouden bij tv-kijken of het spelen van leuke computerspelletjes. Experts vinden dat ouders en leraren ervoor moeten zorgen dat kinderen niet overdreven lang tv-kijken en/of computeren. Ze raden bovendien regelmatig preventief oogonderzoek aan.

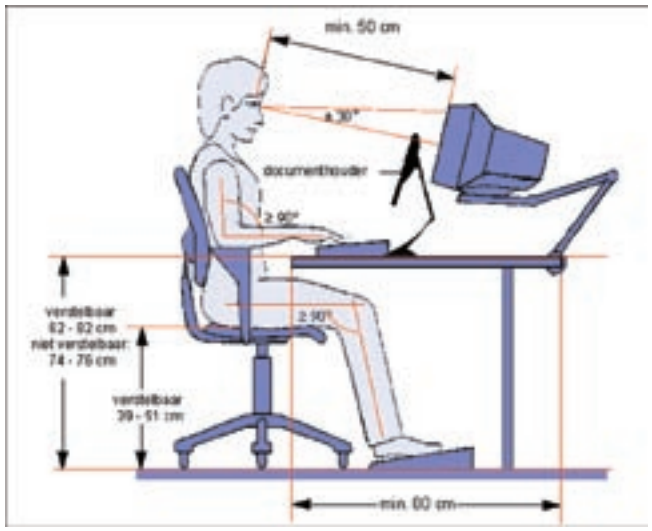
7.4 Wijs op goede houding

Leraren moeten van in de lagere school leerlingen een correcte houding aanleren. De Nederlandse Patiëntenverenging voor RSI stelt op haar website gratis een lessenpakket ter beschikking waarmee leerlingen stap voor stap een juiste houding aanleren (zie lijst hyperlinks na dit hoofdstuk).

Zithouding

Zorg dat de onderbenen verticaal op de grond rusten in een hoek van 90 graden met de bovenbenen. De voeten rusten op de grond. Zit niet met gekruiste benen of schuin gedraaid. Houd je rug recht en laat het onderste deel van de rug tegen de rugleuning steunen. Stel de rugleuning daarop in.

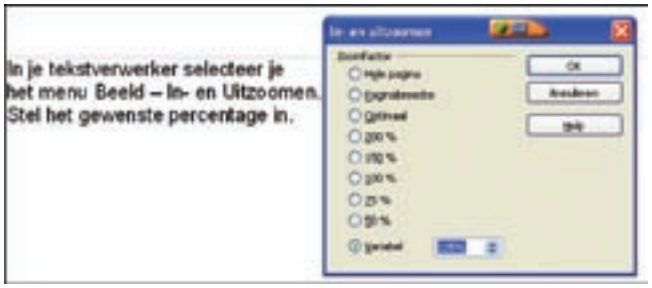
Zit recht voor het toetsenbord en plaats het 8 tot 10 cm van de rand van het werkblad. Klap de pootjes bij voorkeur in omdat je anders gemakkelijk te veel druk legt op de polsen.
Probeer tijdens het typen je polsen recht te houden en laat ze 'zweven' boven het toetsenbord. Buig de pols niet te ver naar achteren. Zorg ervoor dat de armen bij typen voldoende steun hebben van het werkblad of je stoelleuning.



Bron: Nederlandse RSI-vereniging www.rsi-vereniging.nl

Leesbaarheid

Je leest makkelijker donkere tekens op een lichte achtergrond (gebruik lichtgrijs als het scherm met wit te veel flikkering geeft). Zorg dat de letters voldoende groot zijn om gemakkelijk te lezen. Je hoeft daarom niet te typen met een grote puntgrootte. In een tekstverwerker kun je de letters op scherm groter tonen door het instellen van het weergavepercentage bij 'Variabel' (open office) of 'Percentage' (Microsoft Office).



7.5 Heb aandacht voor RSI

Leraren moeten aandacht hebben voor waarschuwingssignalen die wijzen op RSI-klachten. Als een kind bij het computeren over zijn onderarm, elleboog, pols of nek wrijft, dan kan dat een signaal zijn voor mogelijke problemen. Als een rechtshandig kind de linkerhand gaat gebruiken tijdens activiteiten (of omgekeerd), is pijn vaak de aanleiding. Andere signalen? Leerlingen hebben problemen met het oppakken van voorwerpen, laten frequent dingen vallen, vermijden sportactiviteiten of klagen over een doof, pijnlijk gevoel en tintelingen. In die gevallen verwijs je de jongere best door naar een arts of naar het CLB.

Heb je zelf klachten, ook al zijn die nog vaag? Neem dan tijdig contact met een arts. RSI is veel moeilijker te behandelen in een gevorderd stadium. Wat doe je zeker niet? Bij muisarmproblemen in je 'gewone' hand de muis verschuiven naar de andere. In die hand ontwikkel je nog veel sneller RSI-problemen, want je neemt bijna zeker een verkrampte houding aan.

7.6 Meer informatie

Gezond werken
Cd-rom van de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg over gezonde werkomgeving, met o.m. aandacht voor bureaustoelen, bureaus, schermen… Gratis te bestellen op: http://www.werk.belgie.be/publicationDefault.aspx?id=4192

'Ga er eens goed voorzitten', brochure van IDEWE met ergonomische tips voor beeldschermwerkers: www.idewe.be

Informatiewijzer *'Gezond computeren op school'* van ICT op School: www.ictopschool.net/infrastructuur/gezondcomputeren met posters en cartoons voor de klas

Specifieke laptopergonomie:
http://www.Laptopergonomie.nl/ergoinfo.htm.

RSI
Algemene informatie op website Nederlandse Patiëntenvereniging RSI: www.rsi-centrum.nl
'Muisje Max wil geen muisarm' — lespakket voor basisschool in pdf-formaat: http://www.rsi-centrum.nl/doc/muisjemax.pdf

Kleutermuizen
www.kindermuis.nl
www.kleutermuis.nl

.8.

BESCHERM JE COMPUTER TEGEN INDRINGERS

Je computer is een heel nuttig werkinstrument. En bovendien kun je er ook nog leuke dingen mee doen. Dat wil je zo houden. Maar dat lukt niet als je je niet beschermt. Of je nu surft of mailt, je moet rekening houden met veiligheidsrisico's: virussen, spam, spyware, phishing, pharming, misbruik van je wachtwoord of bankrekening, misbruik van je harde schijf of van de rekenkracht van je pc (processorcapaciteit),…

Met je pc op internet zit je pal op de informatiesnelweg. Toen je computer nog niet verbonden was met een netwerk of het wereldwijde web, moest je je alleen indekken tegen een crash van je harde schijf, of een virus dat je via een diskette kon binnenhalen. Nu moet je veel verder gaan.

Op school kun je rekenen op het actieve beveiligingsbeleid van de ICT-coördinator (zie technische informatie voor ICT-coördinatoren). In dit hoofdstuk sommen we de stappen op die je persoonlijk moet nemen om problemen te voorkomen. Dat is tegelijk kant-en-klare informatie om je leerlingen aan te leren hoe zij moeten omgaan met deze veiligheidsrisico's.

Daarbij komen volgende elementen aan bod:

- **(1)** veilige wachtwoorden
- **(2)** firewall
- **(3)** updates
- **(4)** virussen
- **(5)** spam
- **(6)** spyware
- **(7)** phishing
- **(8)** webwinkelen
- **(9)** reservekopies

Dit hoofdstuk sluit rechtstreeks aan bij de tweede eindterm: leerlingen gebruiken ICT op een veilige, verantwoorde en doelmatige manier.

8.1 Veilige wachtwoorden

Is de pincode van je bankkaart nog altijd '1234'? En schrijf je die voor alle zekerheid achteraan op je kaart? Nee toch. En je computerwachtwoord? Is dat de naam van je oudste zoon? Je geboortejaar? De naam van je hond of poes? Je sterrenbeeld? Of je pincode?

Drie basisregels:

(1) gebruik meerdere wachtwoorden;

(2) maak een veilig wachtwoord;

(3) verander je wachtwoord regelmatig.

Meer dan één wachtwoord

Als je slechts één wachtwoord gebruikt voor al je computer- en internettoepassingen, loop je risico's. Want wie er misbruik van maakt, heeft dan niet alleen toegang tot je persoonlijke brievenbus en je gegevens op het school- en thuisnetwerk, maar krijgt misschien zelfs toegang tot je bankgegevens.

Wat doet een kraker?

(1) Hij probeert het wachtwoord op één of andere manier te raden (met voornaam, geboortedatum,…).

(2) Hij installeert een virus (malware) op je pc dat je toetsaanslagen registreert en naar hem doorstuurt.

(3) Hij test met automatische software één voor één alle woorden uit een woordenboek uit.

(4) Hij genereert met krachtige software alle mogelijke combinaties van tekens.

Meerdere wachtwoorden

Kies aparte wachtwoorden voor:

(1) strikt persoonlijke toepassingen zoals je e-mail, bankieren…;

(2) gebruik binnen het netwerk van de school;

(3) websites en toepassingen waar je ook persoonlijke gegevens invoert;

(4) websites en toepassingen waar je occasioneel langs surft.

Pikken webdieven er dan eentje? Dan ben je niet overal bedreigd.

N1etkr@@Kbaar?

Maak het hackers moeilijk. Een veilig wachtwoord? Eentje dat mensen moeilijk kunnen raden en software moeilijk kan kraken. Gebruik daarvoor een wachtwoord met minimum acht karakters:

(1) zowel hoofd- als kleine letters;

(2) een of meer cijfers;

(3) een of meer leestekens/speciale karakters.

Hoe persoonlijker de gegevens waar je met je wachtwoord toegang toe krijgt, hoe veiliger je wachtwoord moet zijn.

Gemakkelijk te onthouden

Bij voorkeur kun je dat wachtwoord ook gemakkelijk onthouden. Dat wordt moeilijk als je een willekeurig gegenereerd wachtwoord als Fe8!KxJ2(gebruikt. Als je het niet meer weet, kun je toepassingen onbereikbaar maken. Misschien blokkeer je dan zelfs de toegang tot je eigen pc of mailbox!

Daarvoor bestaan trucs:

(1) Maak een zinnetje en gebruik daarin de eerste letter van elk woord. > "Ik surf veilig, dus ben ik zuinig met persoonlijke gegevens" wordt dan: isvdbizmpg

(2) Vervang sommige letters door hoofdletters, bijvoorbeeld alle adjectieven > isvdbiZmPg

(3) Vervang bepaalde letters door cijfers, bv. 'i' door '1' of 'e' door '3' > 1svdb1ZmPg

(4) Gebruik leestekens of speciale karakters (bijvoorbeeld de 'a' vervangen door '@') > 1sv,db1ZmPg!

Je kunt ook gewoon vertrekken van een woord. 'Aandachtig' vorm je dan snel om tot: @@nD8t!G.

Wil je zeker weten of je wachtwoord sterk is? Test het online (zie URL's achteraan dit hoofdstuk).

Wil je je wachtwoord écht veilig houden? **Verander** het dan **regelmatig**. Kies voor een totaal nieuw. Of houd het eenvoudiger en gebruik voor andere letters de hoofdlettervariant. Of gebruik nu een uitroepteken in plaats van het getal 1 voor de letter 'i': !Sv;dB1zmpg? is computertechnisch een totaal ander wachtwoord dan: 1sv,db1ZmPg!. Maar wel gemakkelijk te onthouden!

Wachtwoordlogboek

Heb je een reeks wachtwoorden en wil je zeker zijn dat je ze niet kwijtraakt en niet moet onthouden? Gebruik dan software die ze voor je bewaart en in versleutelde vorm opslaat op je computer. Je moet dan slechts één wachtwoord onthouden dat je toegang geeft tot je wachtwoordlogboek. Die pakketten creëren ook veilige wachtwoorden volgens de regels van de kunst.

Password Depot kun je gratis downloaden en als freeware gebruiken. Je hebt dan wel een beperking tot 20 wachtwoorden (www.password-depot.com). Een ander pakket is RoboForm. Het nestelt zich als werkbalk in je browser en bewaart je gebruikersnaam en wachtwoord per website. Het bevat ook een module waarin je identiteitsgegevens kunt opslaan waarmee je formulieren automatisch invult (www.roboform.com). De gratis versie is beperkt tot 10 wachtwoorden. Beide programma's kosten in hun volledige versie minder dan 25 euro.

Straks nog nodig?

Er zijn drie beveiligingsniveaus. Je kunt vertrekken van wat je:

(1) weet: wachtwoord;

(2) hebt: je elektronische identiteitskaart, bankkaart, het federale 'token' dat je gebruikt bij TaxOnWeb;

(3) bent: vingerafdruk, scan van de oogiris.

Elk van deze niveaus is een gradatie veiliger dan het vorige. Daarom stappen bijvoorbeeld banken voor hun e-bankingsoftware af van het wachtwoord en kiezen ze voor systemen met een klein toestelletje dat uw bankkaart inleest en via identificatiecodes de toegang bewaakt en een elektronische handtekening plaatst onder betalingsopdrachten. Ook de elektronische leeromgeving Smartschool start vanaf het schooljaar 2007–2008 met het gebruik van de identiteitskaart voor toegang tot gevoelige bestanden.

8.2 Firewall

Je huis heeft een adres en straatnummer in een gemeente. Je computer heeft een IP-adres om zich te identificeren (vier groepen van maximaal drie cijfers). Maar als gebruiker heb je die nummers niet nodig. Je typt een URL in (www.ond.vlaanderen.be). Op het internet vertalen 'DNS-servers' (domeinnaam servers) die naam naar het juiste IP-adres.

Op het wereldwijde web of het netwerk waarop je inlogt, communiceert je computer met andere computers via het versturen van kleine pakjes 'data'. Die verlaten je computer en komen weer binnen via 'poorten'. Elke pc heeft er ongeveer 130.000. Waar moet jij nu voor zorgen? Dat ongewenste indringers geen poorten misbruiken om in je computer binnen te dringen.

Op school werk je in een netwerk van tientallen computers. Thuis ga je op internet, je ontvangt en verstuurt e-mails. Bepaalde poorten moeten dus openstaan om het gewenste verkeer door te laten. Maar al die andere poorten moet je dicht houden. Je moet ervoor zorgen dat poorten alleen opengaan als dat nodig is om een programma te laten werken.

Persoonlijke firewall

In computerjargon gebruik je daarvoor een **firewall**. Je hebt firewalls die de toegang tot het netwerk op school controleren. Die installeren en beheren is een taak voor de ICT-coördinator (zie technisch hoofdstuk voor de ICT-coördinator). Thuis en op elke computer in een netwerk werk je met een persoonlijke branddeur.

Je hebt thuis een modem die de verbinding maakt met je internetprovider. Sommige modems (vooral draadloze) hebben een ingebouwde firewall die ongewenste gebruikers de weg verspert nog voor ze je computer zelf bereiken. Dat is prima meegenomen.

Daarnaast gebruik je best op je computer een software firewall. Werk je met Microsoft Windows als besturingssysteem? Dan kun je de ingebouwde firewall gebruiken. Heb je voor je bescherming tegen computervirussen (zie verder in dit hoofdstuk) een totaalpakket? Dan krijg je ook daarbij een ingebouwde firewall. Die combinatie is voldoende voor thuisgebruik.

Zorg ervoor dat alle flikkerlichten in het Windows-beveiligingscentrum op groen staan.

Wat doet een persoonlijke firewall?

Die schermt je computer af tegen externe aanvallen. Als je aan de slag bent met een softwareprogramma, zoals een webbrowser of een tekstverwerker, staan er (soms) poorten open. Het programma moet ervoor zorgen dat die poorten niet worden misbruikt. Maar programma's zijn mensenwerk. Er kunnen dus fouten inzitten. Krakers proberen de gaten te vinden en breken zo in. Dat is de reden waarom je programma's regelmatig moet ***updaten*** (zie 1.3), want softwareontwerpers dichten achteraf gaten die bij het gebruik aan het licht komen.

Persoonlijke firewalls controleren of een programma op je computer een verbinding probeert te maken met het internet. Of een poort wil openzetten om anderen verbinding te laten maken met je computer. Bij sommige programma's moet dat: je webbrowser, e-mailprogramma, je tekstverwerker die afbeeldingen zoekt op de website van een leverancier. Maar het is ook mogelijk dat een virus probeert verbinding te maken met internet. Dan moet je die toegang afblokken.

Al doende leren

Een persoonlijke firewall leert al doende. Doe je mee aan spelvormen op internet? Dan is informatie-uitwisseling nodig. Een goede firewall vraagt je dan of je dat programma toegang wilt verlenen. Dan moet je 'ja' zeggen, of je kunt niet gamen. De firewall van je antivirussoftware zal je die vraag ook stellen na bijvoorbeeld een automatische update van je webbrowser.

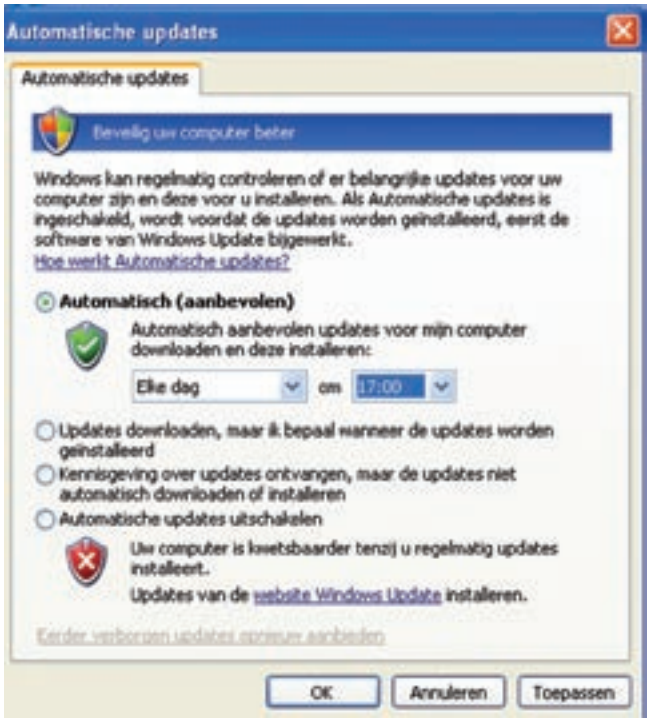
Veel verkeer dat een firewall verdacht vindt, is ongevaarlijk en onschuldig. **Panikeer dus niet bij elke waarschuwing.** Lees aandachtig de boodschap die je firewall op je scherm toont. Gaat het om een betrouwbaar programma? Installeerde je zopas een update? Dan geef je toegang tot de poort. Twijfel je? Weiger dan de toegang, noteer de boodschap en **vraag advies** aan iemand die er meer van weet, bijvoorbeeld de ICT-coördinator op school. Want een weigering kun je achteraf nog omzetten in een toelating. Maar als je een indringer toelaat, zit je misschien wél in de problemen.

8.3 Recentste update

Programma's bestaan uit miljoenen regels programmeercode. Ze zijn nooit 'af'. Regelmatig ontdekken producenten fouten (*bugs*). Dan passen de programmeurs de code aan. Ze stellen de nieuwe versie beschikbaar als een 'patch', een klein programma dat de veiligheidsgaatjes in een programma dicht. Dat overschrijft bepaalde delen van de code, zonder dat je het hele programma opnieuw moet installeren.

Veiligheidsproblemen en bugs doen zich voor in besturingssysteem en toepassingssoftware. Microsoft pakt de meeste problemen effectief aan met *patches*. Die worden verspreid via Windows Update, dat in principe automatisch wordt geactiveerd bij installatie. Je kunt snel controleren of dit het geval is. Ga via 'Start' naar het configuratiescherm. Kies 'Beveiligingscentrum' en kijk of 'Automatische updates' is aangevinkt. Ook de Mac- en Linuxbesturingssytemen gebruiken automatische updates.

Vergeet ook niet de automatische updates van al je software en zeker van je antivirussoftware (zie 8.4) te activeren.



Programmeer de automatische updates op een uur dat je computer normaal ingeschakeld is en verbonden met het internet.

8.4 Virussen

Computervirussen zijn kleine computerprogramma's die zich in een bestand kunnen nestelen, meestal in bestanden van het besturingssysteem. Ze zijn schadelijk omdat ze schijfruimte en computertijd in beslag nemen. In ernstige gevallen richten ze schade aan: bestanden wissen en (gevoelige) gegevens verspreiden. Ze vermenigvuldigen zichzelf en verspreiden zich om zo meer en meer computersystemen te infecteren.

Er zijn virusvormen met specifieke namen.

(1) Trojaanse paarden (Trojan horses) zijn programma's die ongewenst meekomen met (gratis) software die de gebruiker installeert. Ze kunnen wachtwoorden achterhalen, de de computer gemakkelijker toegankelijk maken voor andere virussen, enz.

(2) Wormen zijn virussen die zich zonder tussenkomst verspreiden over computernetwerken, bijvoorbeeld via e-mail.

(3) Een logic bomb is een soort tijdbom die pas schade aanricht op een geprogrammeerd later tijdstip, bijvoorbeeld op Valentijnsdag, op 1 april, of als de ontwerper de bom activeert (bv. een netwerkbeheerder die wordt ontslagen).

Minder, maar niet weg

Virussen halen de twee laatste jaren minder vaak het nieuws. Ze zijn duidelijk op hun retour. Diskettes worden bijna niet meer gebruikt en vooral: de bescherming is enorm verbeterd. Zelfs als er nog een nieuw virus opduikt, heeft het minder impact. Ook het aantal virussen dat via e-mails wordt verspreid neemt af. Een onderzoek van MessageLabs noteerde eind 2005 nog virussen in 3 mails op 100. Eind 2006 was dit gezakt onder de 1 per 100, en het bedrijf voorspelt een verdere daling tot 1 op 300.

Dat heeft ook een nadeel. Virussen zijn niet meer in het nieuws en dat schept een vals gevoel van veiligheid. Want jij zult toch maar die 1 op 300 zijn!

Een firewall (zie 1.2) beschermt je tegen indringers, maar niet tegen virussen. Je moet dus **antivirussoftware** installeren en updaten. Trouwens, de meeste antivirusprogramma's hebben hun actieterrein uitgebreid en helpen je nu ook beschermen tegen spyware, phishing,… (zie verder).

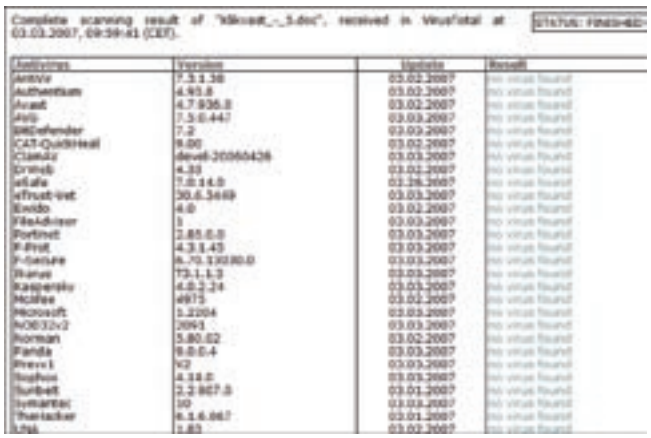
Gratis of betalend

Volledig gratis is de virusbescherming van je internetprovider. De meeste hebben immers zelf antivirussoftware draaien op hun servers en houden heel wat tegen voor de post je brieven-

bus bereikt. Telenet houdt dagelijks een stand van zaken bij en noteert gemiddeld nog een twee miljoen virussen per maand die stranden voor hun filters.

Een goede tip: voer regelmatig een **online virusscan** van je computer uit. Ongeveer elke producent van antivirussoftware biedt dat aan. Let wel: om een gratis virusscan uit te voeren moet je je akkoord geven voor de installatie van een aantal 'ActiveX-controls' in je browser. Bij de standaardinstallatie van een browser als Internet Explorer gebeurt dat niet automatisch — precies om je tegen indringers te beschermen. Ben je daar niet mee vertrouwd of ben je bang voor problemen? Vraag dan iemand om je de eerste keer te helpen.

Vermoed je dat een bepaald bestand besmet is door een virus? Dan kun je dat bestand uploaden naar de website van Virustotal. Daar wordt je bestand gratis gecontroleerd door een heel reeks virusscanners en volg je de resultaten online op je scherm. Je ziet in de figuur hiernaast het resultaat van een online scan van het tekstbestand van dit hoofdstuk. Zo heb je meteen een overzicht van de brede waaier antivirussoftware.



Thuisgebruik

Voor thuisgebruik zijn er een aantal gratis virusbeschermers. De meest bekende is AVG, die je vrij mag downloaden voor persoonlijk gebruik.
De bekendste betalende softwarepakketten voor thuisgebruik zijn: Norton (Symantec), McAfee, Panda en Kaspersky. Een antiviruspakket kost 40 tot 50 euro, de uitgebreidere 'internet security' pakketten kosten ongeveer 70 euro — dan heb je er ook bescherming bij tegen spam, phishing, enz.

WAKker blijven

Toch blijft het belangrijkste wapen tegen virussen je waakzaamheid.

(1) Open geen e-mailbijlagen van onbekende afzenders.

(2) Ook als de e-mail van bekenden komt: open geen bestanden met de extensie .exe of .scr. Twijfel je of de bijlage veilig is? Neem dan eerst contact op met de afzender.

(3) Surf niet naar veelbelovende websites die onbekenden in een e-mail aanbevelen.

(4) Let op met diskettes en USB-sticks (memo- of geheugensticks) van leerlingen: scan ze op virussen voor je de inhoud ervan raadpleegt.

Een **extra voorzorgsmaatregel**? Voer regelmatig de hierboven aangehaalde tip uit: scan je systeem (geheugen en harde schijf) met een online virusscanner. Heel uitzonderlijk misleidt een virus de software en houdt zich schuil gedurende een bepaalde periode om dan toe te slaan. Een externe waakhond vindt die soms wel.

Nepvirus

Af en toe duikelt er een hoax of valse virusmelding in je mailbox. Met wat ervaring kun je die vlug herkennen. Ze gebruiken vaak een alarmerende taal, zoals: 'Het werd zopas gemeld op CNN', 'Microsoft noemt dit het gevaarlijkste virus uit de computergeschiedenis', enz. Bijna altijd bevatten ze een schreeuwerige lijn in hoofdletters, genre: "ONMIDDELLIJK LEZEN EN DOORSTUREN NAAR IEDEREEN DIE JE KENT!!!!!!!".

Trap niet in die val. Verwijder dit soort berichten meteen uit je mailbox. Oók als ze van bekenden komen… Stuur ze in geen geval verder door.

Twijfel je of een viruswaarschuwing nep is? Surf even naar www.nepwaarschuwing.nl. Daar vind je een volledige lijst met alle hoaxes uit de computergeschiedenis.

De 'Rode Lippen'-hoax belandde in december 2005 in duizenden mailboxen.

Afpersers

Een specifieke virusvariant bedreigt je niet alleen met schade aan je gegevens, maar probeert je ook geld af te persen. Het gaat om een 'Trojaans paard'-virus dat zich op je harde schijf nestelt en een aantal bestanden in je map 'Mijn documenten' versleutelt (encrypteert). Een pop-upvenster dreigt ermee de toegang tot het bestand voor altijd onmogelijk te maken, tenzij je een geldsom overmaakt op een bankrekening. Meestal gaat het om relatief kleine bedragen (40 tot 50 dollar of euro). Knap bekeken door de ontwerpers, want die bedragen zijn zo laag dat politiediensten er niet direct echt werk van maken. En vele kleintjes maken toch een groot?

Ook hier is goede virusbeschermingssoftware de oplossing.

Wijs niet met de vinger

Krijg je toch een virus op je systeem en merk je op de schuldige mail een vriend of kennis als afzender? Wijs dan niet meteen met een beschuldigende vinger. Een typisch kenmerk van veel virussen: ze verspreiden zich snel omdat ze automatisch, zonder tussenkomst van de betrokkenen, e-mails verzenden naar alle contactpersonen in het adresboek van Outlook (Express).

Krijg je een e-mail van een bekende mét virus? Neem dan even contact op met die persoon en meld het incident. Met het advies: scan even je computer, want misschien heb je een virus zonder dat je het beseft.

Wees gewaarschuwd

Genees niet, maar voorkom. Dat betekent in de eerste plaats: zorg dat je antivirussoftware zich élke dag updatet.

En abonneer je op de e-mailservice van een erkende organisatie. In België heb je het BIPT (Belgisch instituut voor Postdiensten en Telecommunicatie). Op hun website (www.bipt.be) kun je gratis inschrijven op e-mailwaarschuwingen zodra een nieuw virus zich in België verspreidt. De organisatie Virusalert (www.virusalert.be) is een onafhankelijke organisatie die hetzelfde doet. Wie zich bij hen abonneert, krijgt niet alleen een viruswaarschuwing, maar ook een maandelijkse nieuwsbrief met informatie over computerveiligheid.

8.5 Spam

Diverse onderzoeken wijzen erop dat vandaag meer spamberichten naar de mailboxen stromen dan gewenste mails. Message Labs noteert een gemiddelde van 86,2 % in 2006 (met een groei van 70% in het laatste kwartaal), met andere woorden: meer dan vier e-mail op vijf zijn spam. CleanPort registreert voor april 2007 zelfs een piek van 90,3% en verwacht niet dat dit percentage snel zal dalen. De afzenders zitten vaak in China, Taiwan en Oost-Europa. De nieuwste trend is 'eilandhoppen': spammers gebruiken de domeinextensies van kleine eilanden. Let extra op voor domeinnamen van de eilanden Man (im), Tokelau (.tk), Cocos (.cc) en Tuvalu (.tv). Of ze gebruiken zombie-pc's (zie verder) om deze berichten rond te sturen.

De Deense onderneming ISS verwacht dat spam vooral een grote ontwikkeling zal kennen op het gebied van boodschappen in afbeeldingen. Spam met afbeeldingen heeft een grote kans om door spamfilters te glippen. Het percentage van deze image based spam was begin 2005 minder dan 5 procent van alle spam. Nu ligt dat percentage tussen 40 en 45 procent.

Spam tegenhouden aan de bron

De meeste e-mailprogramma's hebben al een vorm van beveiliging waardoor spamberichten automatisch in een aparte map van je 'Postvak In' terechtkomen. Het is wel aan te raden om

daar af en toe even te kijken: de filters klasseren uitzonderlijk ook eens een gewenste e-mail als spam.

De meeste **internetproviders** filteren zelf al een pak spamberichten. Ze doen dat natuurlijk voor een stuk uit eigenbelang. Als ze alle spam doorlaten, belasten ze hun netwerk overmatig.

Maar het is leuk meegenomen. Meer nog: je hoeft er niets voor te doen. Providers zoals Telenet en Belgacom blokkeren automatisch spamberichten met hun filters. En die werken uitstekend. Telenet heeft trouwens een spammeter op zijn website die bijhoudt hoeveel mails hun filters tegenhouden (per dag, week, maand): interessante informatie voor je leerlingen.

Meer gratis beveiliging

Wil je een sterkere beveiliging? Sommige programma's die je beveiligen tegen virussen, waken ook over spam (meestal zijn het dan pakketten die je koopt als 'totale internetbeveiliging').

Daarnaast zijn er **gratis pakketten**. *Mailwasher* kun je inzetten als programma dat alle e-mails controleert voor ze in je 'Postvak In' belanden (er is ook een meer geavanceerde betalende versie). Je kunt dan afzenders toevoegen aan een zwarte lijst of naar de afzender een bericht terugsturen dat de indruk geeft dat je e-mailadres niet bestaat (in vakjargon: bouncen).

SpamPal maakt gebruik van DNSBL-lijsten. Die brengen in kaart welke delen van het internet spam verspreiden. Als je een e-mail krijgt van een server die op deze lijsten staat, kun je ervan uitgaan dat het een spammail is. Als SpamPal een bericht herkent als spam, dan plakt het een "header" aan dit mailtje. Je moet je e-mailprogramma opdracht geven de berichten met die header in een aparte "spammap" te plaatsen.

Hoe je reageert op spammail die toch in je mailbox belandt, lees je in het hoofdstuk 3 over communicatie.

8.6 Zet Big Brother een hak

Doet je computer vreemd? Werkt je pc trager dan je gewoon bent? Of loopt hij vaker vast? Verschijnen er pop-upadvertenties, zelfs als je niet op het web surft? Zijn de instellingen van je webbrowser plots veranderd? Een andere startpagina of een extra werkbalk? Dan is de kans groot dat er zich spyware in je systeem heeft genesteld. Je gedrag wordt geobserveerd!

Wat is spyware?

Elk programma dat observeert wat je doet op je computer of op het web. Spyware komt voor in verschillende soorten (in stijgende volgorde van risico):

(1) *adware* registreert wat je op het *web* doet om je dan te bekogelen met doelgerichte advertenties via pop-upvensters;

(2) *systeemmonitoren* observeren al wat je op je computer doet: de websites die je bezoekt, chatsessies waaraan je deelneemt, je e-mailverkeer;

(3) *keyloggers* registreren elke toetsaanslag en leggen ook je gebruikersnamen en wachtwoorden vast;

(4) *trojaanse paarden* zijn geen echte spyware maar kleine programma's die zich op je pc installeren en hackers toegang geven tot je pc.

Niet alle spyware is dus gevaarlijk voor je systeem. Sommige is dat wel. Dus: beter te veel beveiligen dan te weinig.

Proef op de som?

Het meeste risico loop je als je gratis muziek downloadt, programma's gebruikt waarmee je bestanden deelt of pornosites bezoekt. Ook wie producten aankoopt via het internet, loopt gevaar om spyware binnen te halen, al is dat dan bijna uitsluitend de ongevaarlijke soort die registreert welk type aankopen je verricht.

Denkt je dat je pc vrij is van spyware? Doe de proef op de som. Surf naar www.lavasoft.com, kies de 'Free Download' en installeer de gratis software Ad-Aware SE Personal. Scan je computer op spyware en verwijder de kritische objecten. Download regelmatig de updates en voer een opkuisoperatie uit met de software.

Let wel: antispywareprogramma's registreren ook niet-kwaadaardige spionnen. Maar het is geen probleem dat je die verwijdert. Bij een volgende bezoek aan je favoriete internetshop, chatbox of spelletjessite duiken die weer je systeem in.

Spyware voorkomen

De beste beveiliging tegen spyware is: nooit downloaden of surfen. Maar dat is natuurlijk geen realistische oplossing. Je kunt wel enkele **veiligheidsvoorschriften** naleven tijdens het downloaden:

(1) download alleen van websites die je kunt vertrouwen;

(2) klik nooit op knoppen zoals 'OK' of 'Agree' om een downloadvenster te sluiten, maar gebruik het rode kruisje rechts bovenaan in het venster (of de toetscombinatie ALT + F4);

(3) wees extra voorzichtig met gratis muziek- en filmbestanden of gratis software.

Geef je privégegevens niet vrij

Virussen zijn op hun retour. Niet te vroeg gejuicht, want een nieuw gevaar dreigt: criminelen proberen je wachtwoorden, bank- en kredietkaartgegevens te pakken te krijgen. Daarmee plunderen ze je bankrekeningen, innen ze je geld voor valse bestellingen of kopen ze producten op jouw naam.

8.7 Phishing en pharming

De nieuwe techniek heet ***Phishing*** – een verbastering van 'fishing', want de hacker 'vist' naar je privégegevens. Een andere methode heet ***Pharming***: de achteloze surfer wordt weggelokt naar een valse website die er net zo uitziet als de originele versie. Het internetadres werd immers gekaapt en omgeleid naar de tijdelijke website van de misdadiger.

Phishing is veel gevaarlijker dan spyware. En recenter. De techniek bestaat nog maar sinds 2001. Pas in 2003 richtten de Amerikaanse banken en andere bedreigde bedrijven de 'Anti-Phishing Work Group' (APWG) op om de strijd aan te binden met deze vorm van computercriminaliteit.

Een eerste rapport van februari 2003 vermeldde 282 aanvallen. In november 2006 telde men al meer dan 37.000 phishing-aanvallen.

INVESTMENT ASSISTANCE

Dear Friend,

I am an Auditor who is willing to place funds in investment opportunities available.

I have certain amount of money I wish to invest in private and start-up companies with potentials for rapid growth in short-terms.

I am interested in placing part of the fund in your company (if any), If by-laws allows for foreign investment. If on the other hand you do not
have a company, I will be happy to listen to any business propositions you may have.

I will like you to contact me through this e-mail :johnsonkema@netscape.net. As well as sending me your company profile (if any) or other necessary informations.

At the meantime, I will appreciate it if you can provide me a few details of yourself . (Full name, age, address and occupations e.t.c)

Please acknowledge the receipt of this mail.

Thanks and God bless.

Your Faithfully,

Johnson Kema.

Een eerste stap in phishing: vertrouwen winnen, bevestiging e-mailadres en persoonlijke gegevens vragen.

Ontfutselen van persoonsgegevens

Ook in 2007 krijgen we te maken met een stijgend aantal phishingmails, sms'jes of chatberichten met als doel persoonsgegevens te achterhalen.
Een malafide link naar perfect geïmiteerde webpagina's vormen dan het lokaas om de ontvanger te verleiden om in te loggen.
Vooral populaire sites zullen door criminelen perfect worden geïmiteerd zoals als eBay, Gmail en bijvoorbeeld websites van financiële instellingen.
Het aantal malafide websites om wachtwoorden te ontfutselen zal in 2007 dan ook in rap tempo toenemen.

Bron: Virusalert

Techniek

De meest gebruikte techniek? je krijgt een e-mail die er heel professioneel uitziet met het logo en de stijl van je bank of internetwinkel. De inhoud? Allerlei smoezen: een storing in het systeem, een vraag naar bevestiging van je klantgegevens, de kans om een superprijs te winnen... Met één constante: de vraag om door te klikken naar een website waar je je persoonlijke gegevens moet bevestigen. Klik je door? Dan kom je op een pagina die er al even professioneel uitziet, maar je wel omleidt naar een valse URL. Meestal merk je dat aan het adres op de statusbalk onderaan: daar staat niet de naam van je bank of webwinkel, maar een andere naam (bv. www.signupaccount.com) of een DNS-nummer (bv. http://172.15.29.13/…).

Een andere techniek is het 'spoofen': het wegkapen van de URL en de bezoeker omleiden naar een valse website. Een voorbeeld? In november 2005 werden heel wat argeloze burgers (die www.google.com selecteerden) omgeleid naar een nepstartpagina van Google. De boodschap? 'U won 400 dollar. Vul je kredietkaartnummer in en wij storten ze vandaag nog op je rekening.'

ICT-beveiliger McAfee ontwikkelde een interessant hulpmiddel om door jou gekozen websites (bv. Surfresultaten) te screenen op spam, spyware, online zwendel en virussen. SiteAdvisor is freeware en kan je gratis downloaden. Je zoekresultaten krijgen dan automatisch een veiligheidsclassificatie groen, oranje of rood. SiteAdvisor is dus geen contentfilter maar waarschuwt alleen over aanwezige malware op een site. Het programma SiteAdvisor is ontwikkeld voor Internet Explorer, maar er is een plug-in voor Firefox.
Zie: http://www.siteadvisor.com

Een aantal tips om niet in de val van criminelen te trappen.

(1) Wantrouw elke e-mail waarin men vraagt naar persoonlijke informatie (gebruikersnaam, wachtwoord, rekening- of kredietkaartnummers). Banken of webwinkels verliezen je gegevens niet en sturen nooit een bevestigingsvraag per e-mail.

(2) Volg nooit een hyperlink in een e-mail van iemand die je niet kent. Typ zelf het adres in of bel eerst naar de afzender om te controleren of de informatie klopt.

(3) Vul in een e-mail nooit formulieren in die vragen naar persoonlijke gegevens (dat mag natuurlijk wel in een formulier op een veilige website).

(4) Vul rekening- en kredietkaartnummers uitsluitend in op beveiligde websites (herkenbaar aan het hangslot in de statusbar en de URL die begint met 'https://' en niet 'http://'.

(5) Log regelmatig in op je pc-banking website (minstens tweemaal per maand) en controleer dan meteen of er geen onregelmatige geldbewegingen gebeurden.

(6) Zorg voor regelmatige updates van je beveiliging tegen virussen en spyware.

Een veilige https-website herken je aan het icoon van het hangslot op de statusbalk onderaan je browser.

Het icoontje met het verbodsteken duidt aan dat je browser automatisch cookies blokkeert.
Het icoontje met het uitroeptaken kun je aanklikken om te controleren of de website geregistreerd is als een phishing-site.

Zombie op een botnet

Misschien het minst bekende gevaar van slechte pc-beveiliging: misbruik van je pc zonder dat je er zelf ook maar iets van merkt. Als een kraker toegang krijgt tot je computer, kan hij hem gebruiken als zombiecomputer. Hij wordt dan op de achtergrond een slaaf van de kraker. Een geheel van zombie-pc's noemt men een botnet of botnetwerk (afkorting van ROBOT NETwork). De beheerder van een botnet heeft de bot herder. Bot herders die een netwerk geïnfecteerde pc's aansturen, 'verhuren' hun botnet tegen tarieven die gaan van 200 tot 50 000 dollar voor diefstal van identiteit en gegevens.

Vaak gaat het om een kraker die een massale spam wil rondsturen. Daarbij heeft hij ten eerste meerdere computers nodig, en ten tweede wil hij niet dat iemand hem kan terugvinden als afzender. Dus verzendt hij de spam via zombie-pc's.

Een tweede gebruik van zombie-pc's: een kraker wil een DDOS-aanval (Distributed Denial of Service) uitvoeren: duizenden of miljoenen pc's proberen op hetzelfde moment dezelfde server te bereiken. Ze willen die uitschakelen zodat de website van dat bedrijf of die organisatie een tijdlang niet bereikbaar is. Of krakers gebruiken je processor en schijfruimte om ingewikkelde berekeningen uit te voeren: jouw pc wordt dus een extra rekenmachine voor ingewikkelde bewerkingen.

Hoe merk je het?

Argwaan is op zijn plaats als je volgende verdachte signalen opmerkt:

(1) onverwachte advertenties nemen je scherm over;

(2) je computer doet alles heel traag;

(3) je antivirusprogramma of firewall weigert dienst;

(4) je kunt niet meer surfen naar de sites van antivirusbedrijven;

(5) de processor is voor 90–100 procent actief (dat kun je controleren in Taakbeheer > Prestaties. Gebruik daarvoor de toetscombinatie Ctrl-Alt-Delete).

Krakers verleiden computergebruikers vaak om een extra programma te installeren dat ze noodzakelijk noemen om de software te installeren. In feite gaat het dan om malafide software die de overname van de pc mogelijk maakt.

CPU geeft het activiteitspercentage van de processor weer. Als u dit soort grafiek krijgt, is uw processor overbelast. Weet je zeker dat komt omdat je veel programma's tegelijk activeerde? Dan is er geen probleem. Gebeurt dit als bijvoorbeeld alleen je e-mailprogramma en tekstverwerker openstaan? Dan is de kans groot dat anderen je processor misbruiken.

Remedie

Zombies zijn met computervirussen of spyware besmette pc's. Je moet ze dus ook bestrijden zoals een computervirus of spyware. Weigert het antivirusprogramma dienst? Dan is de kans groot dat een computervirus het blokkeert. Dan roep je best de

hulp in van iemand met veel computerervaring. Je moet immers eerst een online virusscan uitvoeren via de 'veilige modus' van je Windows-software.

Malware neemt toe

Experts verwachten dat we de komende jaren steeds meer *malware* (verzamelnaam voor phishing, pharming, botnets, enz.) zullen zien verschijnen. Daarbij gebruiken de criminelen een combinatie van spam en 'social engineering'. Hackers proberen in te schatten wat de zwakke menselijke schakel is in het geheel. Zo mikken ze op de nieuwsgierigheid naar het wel en wee van beroemdheden (Britney Spears, Paris Hilton, Jenna Jameson) of nieuwsfeiten. En op de interesse voor sex.

Zo verspreiden ze de malware onder grote groepen mensen waardoor hun kansen op succes aanzienlijk stijgen. Bovendien is het niet nodig een virus als bijlage aan een mail te voegen. Malafide bijlagen worden immers snel door antivirusprogramma's gedetecteerd.

Ze lokken de argeloze gebruiker naar websites die malware op de computer installeren. Daarbij maken ze gebruik van de mogelijkheden die webpagina's bieden om programmeercode uit te voeren. Ze verleiden de bezoeker bijvoorbeeld om een afbeelding aan te klikken. De programmeercode achter de afbeelding start dan een extern programma.

De nieuwste technieken proberen zelfs om de automatische updatefaciliteiten van programma's te misbruiken om zo malware te installeren. Bij een recente studie ontdekte Google dat 10% van de resultaten van zoekacties verwijzen naar webpagina's met ongewenste verborgen software.

8.8 Reservekopie

Een gewaarschuwd man telt voor twee. En zorgt voor twee! Van elk belangrijk bestand moet je (minstens) twee versies hebben: een op je harde schijf en een op een veilige informatiedrager. Gaat het om héél belangrijke informatie? Bewaar dan kopies op twee verschillende plaatsen.

Afgelopen woensdagmiddag werd in de privépraktijk van xx ingebroken. Daarbij zijn een laptop en een externe harde schijf gestolen. Een ramp, want op beide informatiedragers stonden alle bestanden en back-ups van het proefschrift van de fysiotherapeut.

Door de diefstal wordt de onderzoeker zeker een halfjaar tot een jaar teruggeworpen in zijn werk.
"Na vijf à zes jaar studie bevond mijn dissertatie zich in de finale fase. Ik hoopte eind dit jaar, begin volgend jaar mijn doctoraat te verdedigen. Maar nu moet ik een hele hoop opnieuw doen."

(Bewerkt naar artikel in *De Morgen* van 17 februari 2007)

Er kan van alles mislopen met digitale informatie. Een klein ongelukje. Jij (of een van je kinderen…) wist per ongeluk een bestand of een map op de pc, en je vindt niets terug in je prullenmand. Of ingrijpender: je harde schijf gaat stuk, een virus maakt bestanden onklaar, er breekt brand uit,… Of je pc wordt gestolen zoals in het voorbeeld uit het krantenartikel.

Neem kopies

Je kunt dit vermijden door regelmatig kopies te nemen van je bestanden. Wat moet je kopiëren? **Niet de programma's** zelf, want die kun je opnieuw installeren van de originele cd-rom's of opnieuw downloaden. Wel al je eigen werk.

De meeste eenvoudige vorm? Maak een reservekopie op USB-stick, cd of dvd. Gebruik daarvoor een herschrijfbare variant zodat je de bestanden met de recentste versie kunt overschrijven. Gebruik twee cd's of dvd's: eentje voor elke dag (of week als je weinig verandert), eentje per maand of trimester. Bewaar bij voorkeur die tweede versie op een andere plaats (bijv. op school). Waarom? Stel dat het brandt, dat een dief langskomt,… Dan zijn beide versies weg.

Automatiseer

Zeker als je veel met je pc werkt en veel gegevens bewaart op je harde schijf, ben je beter af met een geautomatiseerd proces. Er bestaan verschillende softwareprogramma's die je gratis kunt downloaden. We vermelden er twee.

Taskzip is handig voor bijvoorbeeld maandelijkse back-ups. Dit programma comprimeert de bestanden in een zip-file. Er is wel een beperking tot een maximum van 2 Gb (gigabyte) volume.

Cobian Backup is open source-software en heeft als voordeel dat je een Nederlandstalige versie kunt installeren. Dat vergemakkelijkt het gebruik. Cobian Backup is heel geschikt voor dagelijkse (incrementele) back-ups. Je programmeert de software om in actie te schieten op een ogenblik waarop je pc meestal aanstaat — bij voorkeur een moment dat je bovendien meestal niet aan het werk bent, maar je pc toch aan staat.

8.9 Meer informatie

Internetbeveiliging algemeen
www.ictopschool.net/software/veiligheid
www.saferinternet.be
ludit.kuleuven.be/software/beveiliging/
www.isoc.be
www.internet-observatory.be
veilig.kennisnet.nl/
www.waarschuwingsdienst.nl/

Wachtwoorden
Hoe maak je een wachtwoord?
ludit.kuleuven.be/software/beveiliging/
veiligwachtwoord.uwpc.info/

Controleer de sterkte van je wachtwoord
www.securitystats.com/tools/password.php
www.microsoft.com/belux/nl/athome/security/privacy/password_checker.mspx

Firewall
www.zonelabs.com
www.schoonepc.nl/optim/sygate.html
www.all-internet-security.com/free_firewall_software.html

Antivirusprogramma's
gratis AVG-software: free.grisoft.com
www.mcafee.com
www.symantec.com
www.pandasoftware.com

Virusinformatie
www.bipt.be
www.virusalert.be
www.nepwaarschuwing.nl

Informatie over spam
Spamwebsite van de federale overheid — www.spamsquad.be
Antispamkit van de OESO — http://mineco.fgov.be/information_society (Gevolgen spamming)

Anti-spamsoftware
www.mailwasher.net
www.spampal.org/ (ga naar downloadpagina)

Spywarebestrijders
Ad-Aware — www.lavasoft.com of www.adaware.com
Spamfighter — www.spamfighter.com/Spywarefighter
Windows Defender — www.microsoft.com/athome/security/spyware/software/

Phishing en Pharming
www.antiphishing.org
http://nl.wikipedia.org/wiki/Phishing

Zombies en botnet
www.polfed-fedpol.be/crim/crim_fccu_zombie_nl.php
www.nedbel.be/zombies.htm

Back-upsoftware
Taskzip — http://files.brothersoft.com/freeware/TZip2.zip
Cobian Back-up — www.cobian.se/

In de professionele versie van Windows Vista zit back-up software ingebouwd.

.9.

De ICT-coördinator heeft de opdracht om te waken over het globale veiligheidsbeleid en kan zijn/haar collega's en leerlingen adviseren rond veilig ICT-gebruik.

Vanzelfsprekend zijn alle tips en suggesties die in de vorige hoofdstukken worden vermeld van belang voor visie en aanpak. In dit hoofdstuk groeperen we nog een aantal praktische tips en adviezen voor een samenhangend ICT veiligheidsbeleid.

BELEIDSTIPS VOOR DE ICT-COÖRDINATOR

9.1 Diefstalbeveiliging

In 2005 telde de politie 3.240 inbraken in scholen, in 2004 zelfs 3.592. In het eerste semester van 2006 al 1.786. Heel vaak hebben de dieven het gemunt op PC- en multimediamateriaal. Mits een aantal eenvoudige ingrepen kan elke school een aantal preventieve maatregelen nemen.

De eerste regel kost je niets: plaats computers en dure apparatuur op een veilige plaats. Dat betekent dat je ze niet op de gelijkvloerse en, indien mogelijk, ook niet op de eerste verdieping plaatst. De tweede of hogere verdiepingen hebben de voorkeur omdat die moeilijker bereikbaar zijn. Kies voor een lokaal zonder ramen aan de straatkant. En echt waardevol materiaal, zoals dure beamers, berg je bijvoorkeur op in een lokaal zonder ramen. Geef ook instructies aan het onderhoudspersoneel: ladders en andere klimmateriaal moeten altijd veilig achter slot. Een (energievriendelijke) buitenverlichting met sensor helpt om dieven af te schrikken.

De deuren van de computerklassen hebben een veiligheidsslot. Maakt een collega een sleutel zoek? Overweeg dan of je de cilinders van de sloten niet beter vervangt. Want die sleutel kan ook gestolen zijn. Bij voorkeur plaats je ook een bewegingsalarm in de lokalen. Verwittig dan wel je collega's over de uren waarop het alarm actief is. Leraren durven anders wel eens 's avonds of in het weekend het alarm activeren. Je kunt ook werken met de duurdere oplossing: een alarmmelder in elke computer die automatisch afgaat als het contact met het toestel wordt verbroken (dat kost wel ongeveer 20 euro per toestel).

Laptops

Heb je veel laptops in je computerpark? Opteer dan voor een hechtingssysteem (zogenaamde "notebook locks") met kabels. Of plaats de laptops 's avonds in een stevige en afgesloten kast. Er bestaat ook 'tracking software' die je op de laptop installeert. Via internet kun je dan je gestolen toestel lokaliseren. Er zijn zelfs oplossingen die tracking software combineren met diefstalverzekering en een onuitwisbare hardware identificatie op het apparaat. Dergelijke zaken vind je in de gespecialiseerde computerhandel.

Hou een gedetailleerde inventaris bij van al je computermateriaal met de serienummers van de fabrikant en je eigen inventarisnummers. Breng de eigen nummering samen met naam en/of logo van de school aan op elk toestel. Doe dat met een methode die moeilijk te verwijderen is. Op de cd-rom bij deze publicatie vind je een handleiding voor softwarebeheer van de BSA. Deze handleiding is vooral nuttig voor ICT-coördinatoren en kan gebruikt worden om zowel de commerciële als vrije software op school te beheren.

Gratis preventieve audit

Je kunt een gratis risicoanalyse aanvragen bij de technopreventief adviseur van je gemeente of politiezone. Die analyseert de veiligheid en geeft tips. Doe dat ook voor de school verbouwings- of aanpassingswerken uitvoert. Vaak is de uitvoering dan veel goedkoper. Je kunt de adviseur ook uitnodigen om voor het lerarenteam uitleg te geven over diefstalbeveiliging.

Surf naar www.besafe.be en selecteer in de linkse menubalk 'preventie'. Op basis van de postcode van de school, geeft de website de contactgegevens van de technopreventief adviseur voor uw regio.

9.2 Netwerkbeveiliging

Een van de eenvoudigste en tegelijk belangrijkste beveiligingen waar een school nood aan heeft is: aparte netwerken voor schooladministratie en pedagogisch gebruik door leerlingen en leraren.

Zet je beide op één netwerk? Dan heb je uren werk om beveiligingen in te bouwen. Bovendien zijn dat altijd softwarebeveiligingen en dus kraakbaar. Zeker voor secundaire scholen is dat een risico, want vroeg of laat zit er wel een 'nerd' in een klas die het een hele uitdaging vindt om de schooladministratie binnen te dringen.

Delen leerlingen en administratie dezelfde internettoegang? Installeer de internettoegang dan op de leerlingenserver. Plaats een extra firewall voor de verbinding tussen deze server en die van de schooladministratie.

De beveiliging van het schoolnetwerk begint met de firewall aan de toegangspoort. Pas de beveiliging aan de grootte van het netwerk en laat ze meegroeien. In het vorige hoofdstuk gingen we dieper in op de "persoonlijke" of "lokale" firewall. In dit deel hebben we het over de netwerkbescherming via een netwerk firewall.

Router

De router verbindt het lokale netwerk van de school (LAN of intranet) met het wereldwijde netwerk (WAN of internet). Het is tegelijk de ingang en uitgang van het lokale netwerk, langs waar alle verkeer verloopt. Voor de aansluiting met het internet is een ADSL- of kabelmodem nodig, al dan niet in de router ingebouwd.

De router is dé plaats om de beveiliging van het netwerk te bewaken. De meeste routers zijn dan ook uitgerust met o.m. firewall functies. Duurdere routers hebben meer beveiligingssoftware aan boord. Maar ook een standaard PC, voorzien van twee netwerkkaarten, kan als (bijkomende) router gebruikt worden. Met de geschikte software, ook open source, wordt dit toestel dan een (extra) firewall-, antivirus-, antispam-, proxy-toestel.

Routers worden ook gebruikt om het lokale netwerk in te delen in subnetten. Zo kan je de PC's gebruikt door administratie en directie groeperen in een administratief netwerk, gescheiden van het pedagogisch netwerk waar leerlingen toegang toe hebben. Of een subnet creëren voor het draadloos netwerk, waardoor je je beter kan afschermen van de extra beveiliginsrisico's.

Netwerk Firewall

In de open source omgeving zijn er enkele populaire en degelijke firewall producten, zoals Smoothwall en haar populaire aftakking IPCop (de meest gedownloade firewall op sourceforge.net). Zie ook het artikel over open source firewalls op de bijgevoegde cd-rom.

Stop twee tot vier netwerkkaarten in een PC, download de installatie-CD van IPCop van het internet, en voer de automatische installatie uit. IPCop is een aangepaste Linux versie, maar geen enkele kennis van Linux is vereist. De hele schijf of partitie

wordt in beslag genomen, het toestel wordt immers enkel als firewall gebruikt. In de eenvoudigste versie verbind je met twee netwerkkaarten het lokale netwerk (de "groene" zone in de IP-Cop kleuraanduiding) met het internet (de "rode" zone). Met meerdere kaarten kan je je lokaal netwerk zelfs verder opsplitsen: bv. tussen het administratieve en pedagogische subnet.

Welke PC kan je gebruiken voor een IPCOP firewall? Minimaal een toestel met 128 MB geheugen, voor veel gebruikers en addons wordt minimaal een Pentium 3 met 512 MB aangeraden.

Wie kiest voor "gesloten software", vindt op de markt een rits kant-en-klaar toestellen. Prijzen voor een hardware firewall vertrekken van 1.000 €, met meerprijzen naargelang de opties die je eraan toevoegt. De Belgische producent van hardware firewalls aXs GUARD vermeldt een basisprijs van 5.000 euro voor een volledige bescherming met ondersteuning en updates. De leverancier van ICT-infrastructuur voor onderwijs Sumika biedt al een firewall aan vanaf 1.000 euro.

Links: www.axsguard.com, www.sumika.be

9.3 Automatische updates

Beveiligingsprogramma's hebben nood aan zeer regelmatige (vb. dagelijkse) updates: definities van nieuwe virussen, spyware, beveiligingslekken,… Standaard staan de bronnen hiervoor meestal ingesteld op de servers van de softwareleverancier. Pas de instellingen aan naar een map op een lokale server, en zorg ervoor dat regelmatig op deze map de laatste definities beschikbaar zijn. Zo voorkom je dat bv. 's morgens tientallen of honderden pc's op de internetverbinding staan te drummen om gelijktijdig de bestanden met laatste virusdefinities te downloaden.

9.4 Systeembevriezing

Past het binnen het pedagogisch ICT veiligheidsbeleid van de school dat leerlingen leren omgaan met de instellingen van beveiligingssoftware? Systeembevriezing maakt dit mogelijk, zonder het risico te lopen dat de ICT coördinator voortdurend moet rondlopen om brandjes te blussen…

Wat de leerling ook heeft uitgespookt, een eenvoudig heropstarten wist alle verkeerde handelingen uit als de pc beschermd is met systeembevriezingssoftware, zoals Illusion (van Skanix) of DeepFreeze (van Faronics). Voor alle duidelijkheid: deze programma's bieden géén bescherming tegen bv. verspreiding van virussen als de PC werkzaam is, ze zorgen er enkel voor dat een deze opnieuw opstart zoals oorspronkelijk ingesteld. Beiden laten uitzonderingen toe, zoals mappen waar leerlingen gebruikersgegevens opslaan, en ze kunnen tijdelijk uitgeschakeld worden om nieuwe programma's of nieuwe versie's te installeren.

9.5 Aanvullende bescherming

Tegen Virussen

Gratis virussoftware is voldoende voor een PC die niet in netwerk staat, maar zeker geen sluitende methode om servers te beveiligen. Antivirussoftware:

nl.trendmicro-europe.com
nl.mcafee.com
www.symantec.be
www.pandasoftware.com

Tegen Spam

Tegenwoordig filteren de providers al massa's spammail aan de bron. Maar dat beschermt je zeker niet tegen alle spamberichten. Als bescherming tegen spam installeer je op server- of net-

werkniveau best een professionele versie van Mailwasher (minder dan 50 euro) of een gelijkaardig programma. Dan houd je niet alleen massa's spam tegen, maar heb je ook een duidelijk zicht op wat je tegenhoudt.

www.mailwasher.com
www.spamfighter.com
www.spambully.com

Tegen spyware

Een goede firewall en virusbescherming bieden tegenwoordig al een stevige bescherming tegen spyware. Toch installeer je best ook specifieke software tegen spyware. Het is geen overbodige luxe om pc's regelmatig op te kuisen met de gratis software Hitman Pro. Die onderwerpt de pc aan een analyse door een vijftal pakketten op virussen, spyware, spam, cookies, enz. Neem dan wel je tijd: een analyse door Hitman Pro duurt al snel vier-vijf uur en de analyse gebruikt bijna constant 100% van de processorkracht.

www.hitmanpro.nl
www.lavasoft.com: adaware

9.6 Beveilig e-mailadressen

Bescherm jezelf en je collega's tegen spam: plaats geen exacte e-mailadressen op de website. Want dan zijn ze leesbaar voor mailzoekprogramma's van spamverzenders. Verdoezel het adres, bijvoorbeeld door het at-teken niet te gebruiken zoals info.at-teken.modelschool.be. Of plaats er onzinnige tekens tussen: info!!@!!modelschool.be. Een mens met verstand kan dan het juiste adres intypen, een robot niet.

Wil je echt veilig zijn? Versleutel dan het e-mailadres. IT-expert Karel Titeca van K.U.Leuven stelt een gratis module ter beschikking waarmee je elk e-mailadres laat omzetten naar een aanklikbare, maar toch tegen spamrobotten beveiligde vorm: http://webpalet.titeca.net/securemail.

Meer informatie over het beveiligen van e-mailadressen op websites en weblogs, vind je op: http://guff.szub.net/2005/08/23/email-immunizer.

9.7 Wachtwoordbeleid

Werk je met een server? Dan kun je collega's en leerlingen verplichten om regelmatig hun wachtwoord te wijzigen.

Dat is duidelijk een onpopulaire maatregel. En bovendien bezorgt die je vast extra werk, want je krijgt gegarandeerd een aantal leerlingen en collega's over de vloer die een nieuw wachtwoord instelden en het enkele dagen later niet meer weten.

De maatregel is pedagogisch wel verantwoord. Je verplicht ze aandacht te hebben voor veilige wachtwoorden en voor het belang van regelmatige aanpassing. Nog een argument: als de leerlingen later in een bedrijf werken, is de kans groot dat ze zich moeten inpassen in een beleid dat hen verplicht om regelmatig een nieuw wachtwoord te kiezen.

Op zich is de maatregel doodeenvoudig. Je stelt op de server de periode in dat een wachtwoord geldig blijft. Maandelijks of tweemaandelijks is misschien een beetje te frequent, maar om de vier maanden (ongeveer per trimester) is wel haalbaar. Concreet wordt dat: begin schooljaar, januari en mei.

Dwing je gebruikers ook in de richting van een veilig wachtwoord. Stel bijvoorbeeld in dat het wachtwoord minimum acht karakters lang moet zijn en kleine, hoofdletters en cijfers moet bevatten.

Extra tip: pas het pop-upvenster dat vraagt om hun wachtwoord te wijzigen aan, zodat ze telkens weer de basisregels voor zich krijgen:

- **(1)** minimum acht karakters;
- **(2)** afwisseling van kleine- en hoofdletters, cijfers en bij voorkeur ook speciale karakters;
- **(3)** het belang om dit wachtwoord niet op te schrijven en aan niemand door te geven;
- **(4)** toon een voorbeeld van een wachtwoord dat vertrekt van een zin.

9.8 Beveiliging tegen gegevensverlies: RAID en backup

Je zal het maar meemaken dat je hele boekhouding, je hele archief, alle documenten van school, leerkrachten en leerlingen plots onbereikbaar worden. Alsof de hele kelder met archieven en alle documentenkasten in enkele minuten tijd in vlammen is opgegaan… Beveiliging tegen gegevensverlies door crashes e.a. is een absolute noodzaak.

RAID voor lokale beveiliging

Voor servers is het aangewezen een beroep te doen op RAID (Redundant Array of Independent Disks): verschillende harde schijven worden als één geheel gebruikt, waarbij de informatie met verschillende methodes op meerdere plaatsen opgeslagen wordt.

We beperken ons hier tot twee methodes. RAID-1 is mirroring: twee schijven worden gebruikt en alle informatie wordt tegelijk op beide schijven geschreven. De schijven zijn mekaars "spiegel". Als één schijf crasht, dan is alle informatie te vinden op de tweede schijf. Er zijn wel dubbel zoveel schijven nodig, of anders gesteld, slechts de helft van de totale schijfcapaciteit wordt gebruikt.

RAID is ontstaan in een tijdperk waar goedkope harde schijven erg onbetrouwbaar waren. Men moest dieper in de buidel tasten om harde schijven te kunnen betalen die wél betrouwbaar (genoeg) geacht werden. Informatici van de Universiteit in Berkeley kregen daarom het idee om deze goedkope harde schijven te combineren in een redundante array, zodat óók goedkope harde schijven een betrouwbaar opslagmedium konden vormen. Tegenwoordig zijn harde schijven bedoeld voor de consumentenmarkt stukken betrouwbaarder geworden en beperkt de vraag naar meer betrouwbaarheid en meer snelheid zich niet alleen tot deze markt. Om deze reden is de oorspronkelijke betekenis I in de afkorting RAID gewijzigd van inexpensive (goedkoop) in independent (onafhankelijk).

Bij RAID-5 worden meerdere schijven gebruikt. Bij drie schijven zal een schijf functioneren als de optelsom van de andere schijven. Valt er een schijf uit, dan wordt de vervangende harde schijf opnieuw beschreven met de informatie van beide andere. RAID-5 gaat economischer met de totale schijfcapciteit om dan RAID-1, maar vraagt meer rekenwerk van de schijfcontroller.

Reservekopie (Backup)

Een RAID oplossing helpt niet als een probleem zich niet beperkt tot één schijf, maar een hele server of een lokaal of een gebouw: brand, waterschade, diefstal, bij vergissing verwijderde gegevens,… Hier zijn reservekopieën nodig die op een andere plaats (een ander gebouw of thuis) bijgehouden worden. Net zoals je best het netwerk opsplitst in een educatief en administratief subnet, is het aangewezen van elk een eigen backup systeem bij te houden.

Tape is het klassieke medium voor reservekopieën, maar de algemene verspreiding van goedkope CD en DVD writers en schijfjes biedt meer flexibiliteit. Ook het huidig aanbod van externe harde schijven maakt archivering en reservekopieën gemakkelijker. Via het lokaal netwerk van de school, of zelfs via het internet, kunnen online reservekopieën gemaakt worden in andere gebouwen.

Backup software is standaard aanwezig in Windows en wordt meestal meegeleverd met harde schijven. Andere bronnen voor backup software:

- www.sourceforge.net, de verzameling van open bron projecten
- backup.startpagina.nl
- tucows.com/Windows/IS-IT/FileManagement/BackupRestore/

Regelmatigheid van backup

Als je elke dag een reservekopie maakt en daarbij de voorbije versie overschrijft, dan kan je maximaal op de gegevens van een

dag geleden terugvallen. Soms is het echter nodig de situatie van enkele dagen geleden of van een maand geleden te kunnen opvragen.

Een eenvoudige maar voldoende methode is de volgende:

Neem een automatische dagelijkse backup per (werk)dag van de week: dus op maandag overschrijf je de backup van de vorige maandag, enz… Je kan daardoor terugkeren naar de gegevens van gisteren, of eergisteren,… tot een week geleden.

Neem een manuele kopie na elke belangrijke administratieve of pedagogische periode: inschrijvingsweken, examenperiode, jaarafsluiting. Deze kan je best archiveren (dus niet meer overschrijven) en dubbel aanmaken, zodat je het archief kan spreiden over twee plaatsen.

9.9 Beperking internettoegang

Vooral in het technisch- en beroepsonderwijs hebben leerlingen heel wat vakken in de computerklas, zoals boekhouden, informatica, tekstverwerking. Vaak staat de leraar vooraan uitleg te geven en ziet hij de schermen van de leerlingen niet. Die durven dan wel eens wat anders doen dan meewerken in de les: spelletjes spelen of surfen.

Vaak erg vervelend voor de leraar. Soms merkt hij duidelijk dat leerlingen met wat anders bezig zijn en moet hij er de les voor onderbreken. En leerlingen zijn nu eenmaal supersnel in het switchen van scherm en dan kan de leraar ze niet meteen betrappen.

Een aantal scholen werkt daarvoor met een stukje javascript in de browser. Leerlingen krijgen dan elk uur een nieuw wachtwoord waarmee ze een uur lang toegang hebben tot internet. Wil een leraar een surfvrije les? Dan geeft hij het wachtwoord dat lesuur niet door. De leraar vindt telkens het wachtwoord op de lerarenpagina's. Daar zitten ze veilig beschermd door zijn persoonlijk toegangswachtwoord.

De zwakke plek van deze beveiliging is duidelijk: leraren mogen nooit het wachtwoord vrijgeven waarmee leerlingen toegang krijgt tot het tekstbestand. Want dan gebruiken ze dat ook in andere lessen. En dat wachtwoord verspreidt zich razendsnel door de gangen!

Het is dus belangrijk dat je dit soort maatregel niet van bovenaf doordrukt, maar bespreekt met directie en collega's. Het systeem werkt alleen als iedereen er zich achter zet.

9.10 Volledige klas- en schermcontrole

Je kunt natuurlijk verder gaan en een volledig trainingprogramma installeren. Twee gekende voorbeelden zijn Net Op School en NetSupport.

Daarmee kan de leraar zijn scherm projecteren op dat van elke leerling en demonstraties geven. Omgekeerd kan de leraar zijn leerlingen aan het werk zetten. Op zijn console ziet hij verkleinde weergaven (thumbnails) van alle schermen in de klas. Wil hij een leerling in detail volgen? Dan vergroot hij dat scherm. Wil hij een leerling tonen hoe hij iets moet doen? Dan blokkeert hij even de muis en het toetsenbord op de leerlingcomputer en neemt zelf de besturing over.

Het programma bevat ook uitgesproken elementen van beveiliging. De leraar kan het browsen beperken tot een selectie websites die hij selecteert. Kwestie van te garanderen dat ze in de aardrijkskundeles alleen met geografische informatie bezig zijn bijvoorbeeld. De leraar kan van op zijn console ook zien welke programma's een leerling heeft openstaan. Spelletjes of een webbrowser tijdens de les boekhouden worden zo van op het lerarenbureau gedetecteerd. De leraar kan ook een of alle computers vanaf zijn console afsluiten.

Er zijn ook didactische extra's aan verbonden, zoals de mogelijkheid om aan het einde van de les een automatisch verwerkte toets af te nemen. De leraar kan zijn scherm ook gebruiken als whiteboard waarop hij uitleg geeft. Stelt hij een vraag en weet de leerling het antwoord? Dan geeft hij de controle even door en kan de leerling zijn antwoord tonen aan de hele klas. Zonder dat hij zijn plaats verlaat.

Dit is software die het lesgeven versoepelt. En het biedt leraren extra hulpmiddelen om controle te houden over de les. De kostprijs is niet onoverkomelijk. Rond 50 euro per licentie het eerste en minder dan 10 de daarop volgende jaren.

www.netopnl.com
www.netsupport.nl

9.11 Beveilig de leeromgeving

Nog regelmatig hoor je berichten over scholen waar een leerling een bericht stuurt naar alle gebruikers van het elektronische leerplatform en via die weg een andere leerling pest. Of het wordt gebruikt om racistische of discriminerende berichten rond te sturen.

Nochtans kun je in elk elektronisch leerplatform de optie uitschakelen waarmee een gebruiker berichten kan versturen naar alle leden. Die optie kan zinvol zijn voor de directie en uzelf. Maar laat ze niet openstaan voor om het even wie. Een eenvoudige manier om heel wat probleemsituaties te voorkomen. Ook de forumfunctie kan je uitschakelen. Een te overwegen optie als de leraars het forum niet voor didactische redenen gebruiken.

Weet je niet hoe dat moet? Vraag vandaag nog advies aan de leverancier van je elektronisch leerplatform.

Stel de browsers in de pc-klassen zo in dat het geheugen gewist wordt als de leerling de browser afsluit. Dat is een uitstekende aanpak. Niet alleen verhinder je zo dat leerlingen kunnen profiteren van het werk van voorgangers. Je wist meteen alle sporen van eventuele pornografische of racistische websites die een leerling bezocht en waarvan hij sporen naliet.

Activeer op elke browser de pop-upblokkering en stel de beveiliging in op hoog (zeker in basisonderwijs en eerste graad secundair) of gemiddeld. Desactiveer het automatisch invullen van wachtwoorden en het downloaden van Activex controls.

9.12 Inhoud website

Meestal ben je als ICT-coördinator ook webmaster. Dan ben je ook verantwoordelijk voor de inhoud van de schoolwebsite.

Als je die opdracht beheersbaar wilt houden, moet je ervoor zorgen dat je alleen publiceerrechten voor de website geeft aan collega's op wie je volledig kunt betrouwen. Spreek met hen duidelijk af dat ze de inhoud van alle pagina's voor publicatie goed moeten screenen. En stel een overeenkomst op waarin ze de verantwoordelijkheid voor hun onderdeel van de website op zich nemen.

Controleer op:

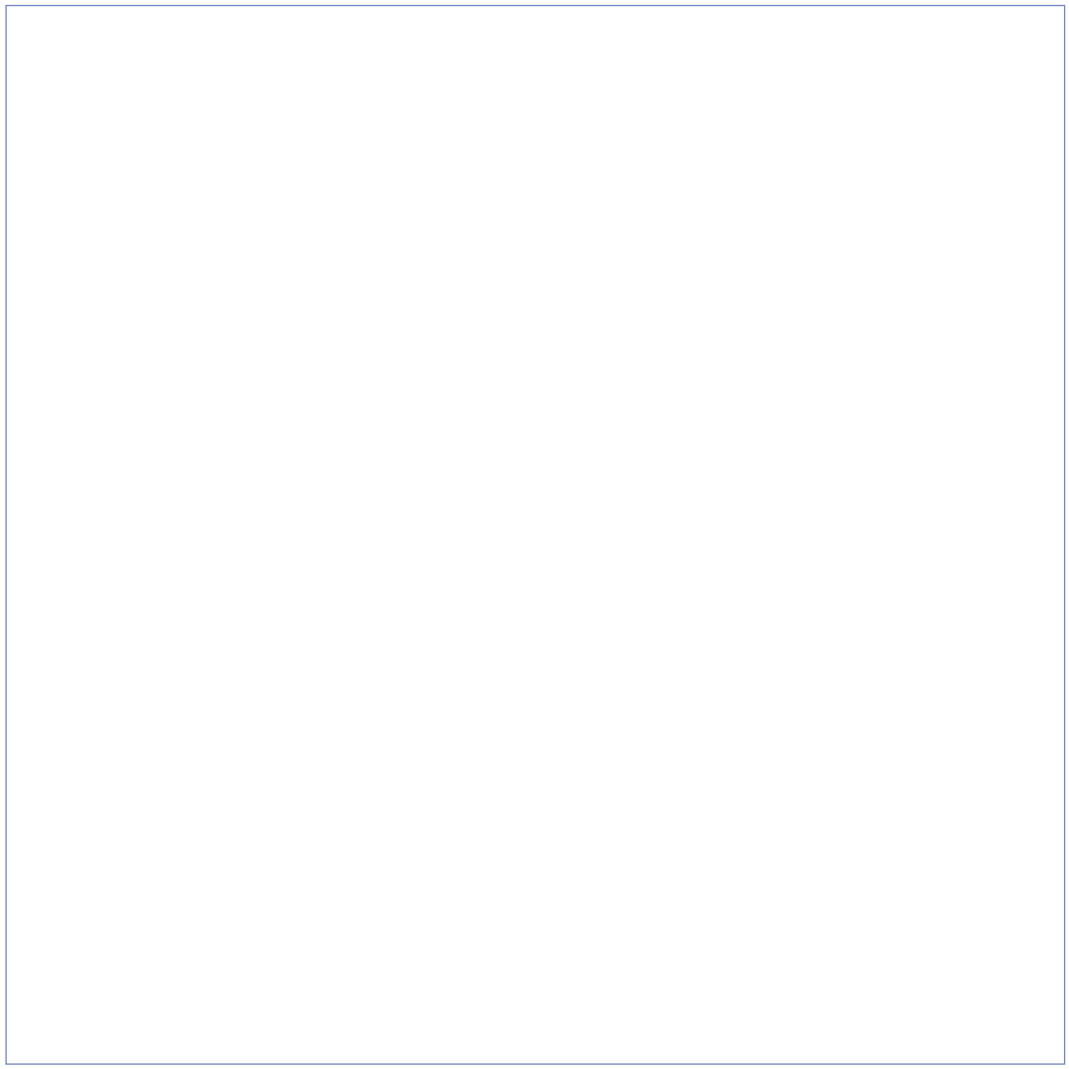
- **(1)** het naleven van het auteursrecht;
- **(2)** het respecteren van de wet op de bescherming van de persoonlijke levenssfeer – plaats alleen foto's als je het schriftelijke akkoord hebt van de ouders van minderjarige leerlingen en van de meerderjarigen zelf die op foto's staan;
- **(3)** beledigende, racistische, discriminerende of negationistische uitlatingen;
- **(4)** compromitterende beelden.

Plaats op de website van de school een formulier waar leerlingen anoniem kunnen melden als ze in de schoolcontext worden geconfronteerd met uitingen van cyberpesten, vandalisme, racisme, discriminatie, compromitterende beelden.

9.13 ICT-protocol

De beste bescherming tegen vandalisme is nauwlettend toezicht van alle leraren op basis van een protocol voor het gebruik van de pc-klassen. Daarin leg je vast dat elke leerling bij het begin van een sessie in de pc-klas moet controleren of de apparatuur volledig in orde is. Is er een probleem? Dan moet hij dat direct melden aan de begeleidende leraar. Doet hij dat niet en meldt een leerling na hem het probleem? Dan is hij verantwoordelijk. Je vindt een voorbeeld van een protocol op de cd-rom bij dit boekje.

CD-ROM



Deze cd-rom kan u raadplegen op elke pc met een internetbrowser (Internet Explorer, Firefox, Safari etc.). De cd-rom start normaal vanzelf op. Zoniet, dan kan u de cd-rom opstarten door te dubbelklikken op index.html of via uw verkenner. De software om pdf-documenten te lezen vindt u ook op deze cd-rom.

Wij wensen een aantal personen in het bijzonder te bedanken voor de medewerking die zij hebben verleend aan deze publicatie. Vooreerst de leden van de redactieraad - Tom Van Renterghem, Fernand Mesdom, Sandra Termont, Mark De Quidt en Stefaan Hendrickx -die de ontwikkeling van de tekst kritisch hebben opgevolgd en aangevuld met waardevolle tips, teksten en suggesties. Tenslotte willen we ook onze waardering uitdrukken voor de bereidwilligheid waarmee diverse organisaties hun medewerking hebben verleend aan deze publicatie, met name Sensoa, Child Focus, de Business Software Alliance, het Onderzoeks- en Informatiecentrum van de Verbruikersorganisaties, Remco Pijpers van de Stichting Mijn Kind Online, het Centrum voor Gelijkheid van Kansen en Racismebestrijding, Klasse, MMG Film en TV-producties, Prof. Dr. Michel Walrave, de Nederlandse RSI-vereniging en Adobe Belgium.

Colofon

Samenstelling en productcoördinatie
Jan De Craemer

Verantwoordelijke uitgever
Micheline Scheys
Afdeling Beleidscoördinatie Onderwijs
Koning Albert II-laan 15
B-1210 Brussel

Redactie
Jaak Poot
www.schrijfdirect.be

Vormgeving
helena.be bvba
Levi Seeldraeyers & Emanuel Maes
www.helena.be

Druk
Drukkerij Vanden Broele
www.vandenbroele.be

Realisatie cd-rom
Develop-IT
www.develop-it.be

Depotnummer: D/2007/3241/179

Deze publicatie kwam tot stand i.s.m.