ouder-handleiding

Leer uw kinderen veilig internetten

ins@fe

DIGI bewust

Gesteund door: upc

INHOUD

A. Hoe gebruikt u dit pakket

Als je een jaar vooruit plant, plant dan rijst.
Als je tien jaar vooruit plant, plant dan een boom.
Als je een leven lang vooruit plant, onderwijs dan je kind
Chinees gezegde

Beste ouder/verzorger,

Voor u ligt het e-safety-pakket voor gezinnen met kinderen tussen 6 en 12 jaar. Dit leermiddel is tot stand gekomen vanuit de overtuiging dat nieuwe technologieën geen kloof moeten veroorzaken tussen generaties, maar hen juist moeten samenbrengen. Het is samengesteld met de expertise van Insafe, het pan-Europese netwerk van nationale contactcentra die het bewustzijn rond veilig internetten willen vergroten. In Nederland is Digibewust het nationale contact centrum en draagt in die hoedanigheid zorg voor de verspreiding. Dit e-safety-pakket is ontwikkeld en tot stand gekomen met de steun van UPC.

Net zoals spelen in de speeltuin of de straat oversteken gevaarlijk kan zijn als je niet oplet, kan het gebruik van internet en mobiele technologieën ook gevaarlijk zijn als je niet voorzichtig bent. Gelukkig bestaan er middelen waarmee internetgebruikers zich op de hoogte kunnen stellen van de zowel de voordelen als de risico's van surfen op het web.

Gebruik dit nieuwe pakket om uw kinderen te helpen bij het leren om veilig en efficiënt gebruik te maken van het internet. Het pakket bevat ruim vijftig veiligheidstips en oefeningen waarmee uw kinderen op een leuke, plezierige en niet-bedreigende manier kunnen kennismaken met e-safety. Het pakket bevat:

- Twee boekjes over e-safety: een gezinsgedeelte en een ouderhandleiding;
- Hoofdregels;
- Een gezinscertificaat;
- Een stickerset;
- 12 kaartjes met verschillende situaties die de kinderen kunnen uitknippen.

Zowel het gezins- als het ouderboekje zijn voorzien van kleurencodes om vier belangrijke e-safety-thema's te belichten: Beveiliging, Communiceren, Entertainment & Downloaden en Digitaal pesten. Het ouderboekje dient als naslagwerk voor het gezinsgedeelte: het bevat achtergrondinformatie, aantekeningen bij de activiteiten en voorgestelde oplossingen voor bij de oefeningen en de situatiekaartjes.

Het is de bedoeling dat het gezinsboekje door de kinderen en de ouders samen wordt gebruikt. De vier thema's worden besproken aan de hand van een verhaal over twee kinderen, Alex en Zeta, hun ouders en de IT-expert, Hedwig. Elk hoofdstuk bevat leerzame activiteiten, zoals online oefeningen, toetsjes, hoofdregels en handige links.

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

Als uw kinderen zich succesvol door het pakket hebben heen gewerkt, kunt u ze belonen door iedereen het gezinscertificaat te laten ondertekenen en een aantal hoofdregels af te spreken. Tot slot kunnen uw kinderen de boekjes nog versieren met de emoticonstickers.

Uw commentaar is waardevol voor ons. Schroom niet bij vragen of opmerkingen contact met ons op te nemen. We wensen u en uw gezin veel plezier bij het controle krijgen over het internet!

Veel veilige surftochten gewenst,

insafe DIGIbewust

1. Beveiligd en wel

EEN COMPUTER IN HUIS

Een computer kan heel leerzaam en ontspannend zijn voor het hele gezin. Door de computer in een gezamenlijke ruimte te zetten en specifieke afspraken te maken over de speeltijd en de voorwaarden waaronder de jongere gezinsleden de computer mogen gebruiken, houdt u het veilig voor ze.

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

UW COMPUTER BEVEILIGEN

Een veilige omgeving kan worden bereikt door een fundamenteel inzicht in potentiële gevaren en kennis van eenvoudige oplossingen. Tot die oplossingen behoren nuttige technologische

hulpmiddelen en het gezonde verstand van de gebruiker. Net als andere zaken ontwikkelt gezond verstand zich met de jaren en door ervaring op te doen.

Het gebruik van **geheugensticks** of **cd-roms**, het openen van **bijlage**n en downloaden van bestanden kunnen gevaarlijk zijn. Die gevaren hebben voornamelijk betrekking op kwaadaardige **computerprogramma**'s (**malware**) die zijn ontworpen om uw computer schade toe te brengen, persoonlijke gegevens te stelen of ongevraagd reclame te sturen.

De kinderen maken kennis met diverse soorten malware: **virus**sen, **worm**en, **Trojaanse paard**en en **spyware** en leren de symptomen van een geïnfecteerde computer te herkennen. Ze leren hoe ze besmetting kunnen voorkomen door altijd alleen het internet op te gaan op een computer die is beschermd met bijgewerkte **antivirus**- en **antispyware**programma's. Ze worden ook aangeraden om voorzichtig te zijn als ze e-mailbijlagen van onbekende afzenders openen, programma's van het internet downloaden en USB-sticks of cd-roms gebruiken.

SPAM BESTRIJDEN

80% van alle e-mails die op het internet circuleren, is **spam** (ongewenste e-mail) waar uw kinderen makkelijk mee te maken kunnen krijgen. Het onoplettend op het **web** publiceren van een **e-mailadres** bij het gebruik maken van een **nieuwsgroep**, **chat**site, een openbaar **forum**, een **social networking**site of een **online formulier** kan spam tot gevolg hebben. Specifieke software kan e-mailadressen verzamelen van het web om adressenlijsten samen te stellen die vervolgens worden gebruikt om in enorme hoeveelheden spam te verspreiden. De bedrijven die zich met dergelijke activiteiten bezighouden, zijn vaak gevestigd op plaatsen waar geen wetgeving bestaat tegen ongevraagde e-mail.

Spam heeft vaak betrekking op pornografie, farmaceutica, dubieuze financiële transacties etc. Bovendien kan spam ook de bron van kwaadaardige programma's zijn. Meestal wordt spam verspreid met frauduleuze bedoelingen. Hieronder volgen enkele tips om uw gezin te beschermen:

- Gebruik **spamfilter**s. Uw e-mailaanbieder biedt doorgaans antispamfuncties aan die u in uw e-mailprogramma kunt activeren. Vraag uw e-mailaanbieder om meer informatie. Controleer regelmatig uw **junkmail**- of **spammap** om te kijken of daar geen onschuldige e-mails in zijn terechtgekomen. Technologie is niet onfeilbaar.
- Leer uw kinderen geen e-mail van onbekenden te openen. Spam bevat bijna altijd uitnodigende aanbiedingen en bijlagen. Laat ze zien hoe je de afzender van een e-mail moet blokkeren of vraag ze verdachte e-mails gewoon te verwijderen.

SURFEN OP HET NET

Zelfs voor heel jonge kinderen kan het nuttig zijn om voor de lol op het internet te surfen en leerzame **website**s te bezoeken. Er staat echter ook allerlei inhoud op het internet die niet altijd geschikt is voor jonge surfertjes.

Met zoekmachines kun je uitstekend informatie zoeken op het internet. Maar omdat het zoeken afhankelijk is van de gekozen zoektermen kun je ook al snel ongewenste inhoud tegenkomen. Een onschuldig klinkende zoekterm kan een niet zo onschuldige website opleveren die de zoekterm in kwestie bevat. Hieronder volgen enkele tips om uw kinderen veiliger te laten surfen op het internet:

- Maak met een **besturingssysteem** (bijv. Windows, Linux, Mac OS) een speciale gebruikersaccount voor uw kind waarop u een functie voor **ouderlijk toezicht** kunt activeren;
- Ga de functies voor ouderlijk toezicht op uw **internetbrowser** en zoekmachine na. Zorg dat u op de hoogte bent van de keuzes die de **gezinsinstellingen** van deze middelen u bieden;
- Stel voor de jongere internetgebruikers in uw gezin kindvriendelijke **zoekmachine**s voor. Bijvoorbeeld http://kids.yahoo.com, http://www.davindi.nl;
- Sla de adressen van de websites die uw kinderen het meest gebruiken op in hun map **Favorieten** (een browserfunctie) of gebruik en speciale kinderbrowser. Zo kunnen ze steeds weer naar hun favoriete sites op het **net** zonder een zoekmachine te hoeven gebruiken.

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

Filters kunnen zodanig beperkend werken dat ze onschuldige inhoud blokkeren. Kinderen kunnen dan bijvoorbeeld geen informatie over de Tweede Wereldoorlog opzoeken voor een geschiedeniswerkstuk, omdat die zoektocht naar websites leidt waarop geweld wordt beschreven. Bovendien, een filter die kan worden geactiveerd, kan ook weer worden gedeactiveerd door slimme jongeren die vaak meesters zijn in het uitwissen van hun sporen. U komt hier alleen achter als u zelf leert hoe u de computer en de software moet gebruiken.

Bezoek de website van **SIP-Bench**. Deze door de Europese Commissie gesteunde studie heeft 30 hulpmiddelen voor ouderlijk toezicht en antispamhulpmiddelen getest op hun doeltreffendheid om kinderen tussen 6 en 16 jaar te beschermen tegen schadelijke inhoud van diverse internettoepassingen: **browsen**, e-mailen, **bestanden versturen**, chatten en **instant messaging**.

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

HOOFDREGELS VOOR OUDERS VAN SURFENDE KINDEREN

- Zorg dat uw computer is beveiligd met een **firewall** en antivirus- en antispywaresoftware. Houd deze up-to-date en let op eventuele **alarmsignalen** die ze geven. Controleer of uw internetaanbieder antivirus- en antispywarehulpmiddelen aanbiedt die u kunt gebruiken;

- Gebruik een spamfilter op uw e-mailprogramma en houd uw e-mailadres zoveel mogelijk voor uzelf door het niet op het web te publiceren. Mijd e-mails van onbekende afzenders en scan bijlagen voordat u ze opent;
- Benut zoveel mogelijk de functies voor ouderlijk toezicht van uw besturingssysteem, internetbrowser, zoekmachine en e-mailprogramma. Maak aparte **gebruikersaccount**s voor uw kinderen. Stel privacyinstellingen zo hoog mogelijk in (ga naar het menu "Extra" in uw browser);

- Overweeg aanvullende filtersoftware te gebruiken;

- Neem als uw computer zich vreemd gedraagt direct contact op met uw internetaanbieder of een expert: uw computer kan geïnfecteerd zijn. Uw internetaanbieder moet ook advies voor ouders kunnen geven;

- Stuur een rapport aan uw nationale internet**meldpunt** (zie Handige links) als u online ongewenste inhoud tegenkomt;

- Ga zo vaak mogelijk bij uw kinderen zitten als ze aan het surfen zijn. Dit is een uitstekende manier om een discussie te stimuleren en het vertrouwen te vergroten. Maak er een uitdaging van om samen te leren;

- Onthoud dat deze veiligheidsregels zowel op u als uw kinderen van toepassing zijn. Moedig hen aan het u te vertellen als ze vreemde dingen tegenkomen.

HANDIGE LINKS

Om veilig te kunnen surfen, is kennis essentieel: weten wat de risico's zijn, weten hoe u zichzelf kunt beschermen en nog meer kennis opdoen. Kijk voor meer informatie op de website van Digibewust *http://www.digibewust.nl*

Als u tijdens het surfen inhoud tegenkomt waarvan u vermoedt dat die illegaal is, kunt u dit melden bij het Meldpunt Kinderporno op internet: *http://www.meldpunt-kinderporno.nl* Jongeren kunnen terecht op *http://www.helpwanted.nl*

Actuele informatie, handreikingen en links over veilig internetten en computerbeveiliging voor ouders, leraren, kinderen, scholieren is te vinden op *www.kennisnet.veilig.nl*

Op *www.iksurfveilig.nl* staat het Diploma veilig internet, ontwikkeld om kinderen bewust te maken van de gevaren en het eigen handelen op internet.

Op surfsafe.nl leren kinderen hoe zij veilig moeten omgaan met internet. Door de quiz in te vullen is te zien hoe veilig uw kind surft. *http://www.surfsafe.nl*

Een gratis kinderbrowser vindt u op *www.mybee.nl*

Kijk als ouder ook eens op *www.mijnkindonline.nl* en *www.kinderconsument.nl*

2. Communiceren

PUZZELSTUKJES

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

Het hoofdstuk over communiceren laat ouders en kinderen kennismaken met begrippen als **persoonlijke gegevens**, **privacy**, positieve online interactie en het omgaan met risico's, zoals contact met vreemden. Online privacy hangt zeer nauw samen met **account**s & **profiele**n. Met een account krijgt u toegang tot een online dienst.

In de echte, offline wereld bevat een busabonnement, een abonnement op de sportschool of een lidmaatschapskaart persoonlijke informatie over u. Online accounts en diensten zijn daarmee te vergelijken. Je kunt van geen van beide gebruikmaken zonder enkele persoonlijke gegevens te verstrekken die worden gebruikt om uw gebruikersprofiel aan te maken. Het is van belang om te weten dat u zelf kunt bepalen welke informatie u over uzelf ter beschikking stelt en met wie u deze informatie wilt delen.

Uw privacy beschermen is een kwestie van bepalen wat u mensen over uzelf wilt vertellen, en niet van liegen over uw identiteit. Jongeren zijn enthousiast over het online communiceren met vrienden en het creëren van hun online imago. Ze staan echter niet altijd stil bij de gevolgen van het openbaar maken van persoonlijke informatie.

EEN PROFIEL AANMAKEN

De eerste stap in het beschermen van persoonlijke informatie is het aanmaken van een veilig profiel door zorgvuldig na te denken over de gegevens die erin komen te staan en de privacyinstellingen die u wilt toepassen.

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

Houd **wachtwoord**en van accounts altijd geheim. Zorg ervoor dat uw kinderen begrijpen dat ze

hun persoonlijke accounts niet moeten delen met vrienden die mogelijk misbruik zouden kunnen maken van hun vertrouwen. Aan de andere kant kan het goed zijn dat u de wachtwoorden van uw kinderen wel weet, zodat u toezicht kunt houden op hun accounts: praat hier over met hen.

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

Als uw kinderen gebruikmaken van chatrooms ga dan na of:

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

FOTO'S EN WEBCAMS

Kinderen moeten inzien dat hun foto een wezenlijk deel uitmaakt van hun privacy en dat digitale afbeeldingen zeer invloedrijk zijn. Ze zijn makkelijk te verspreiden en te **bewerken**, en zeer moeilijk te wissen wanneer ze eenmaal via een computer of mobiele telefoon zijn verstuurd: ze kunnen heel lang online blijven staan! **Webcam**s moeten met de nodige voorzichtigheid worden gebruikt en kinderen dienen de webcam niet zonder toezicht te gebruiken. Hulpmiddelen en **directories** voor chatten met een webcam kunnen riskant zijn. U en uw kinderen dienen persoonlijke afbeeldingen alleen te delen met mensen die u kent en vertrouwt: vraag altijd toestemming voordat u een foto van iemand anders publiceert. Laat uw kinderen geen computer en webcam gebruiken als ze alleen op hun kamer zijn.

CONTACT MET VREEMDEN

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

Uw kinderen kunnen diepe vriendschappen opbouwen met online vrienden. Maar ze hebben ook de neiging om mensen die belangstelling voor ze hebben en begripvol zijn makkelijk te vertrouwen, zelfs als ze deze mensen niet zo goed kennen. Daardoor kan de verleiding groot zijn om in het echt met die nieuwe vrienden af te spreken zonder dat ze u hierover vertellen. Kinderen zijn zich vaak niet bewust van het gevaar van zulke afspraken en kunnen die als niet belangrijk beschouwen. Dit maakt hen makkelijke prooien voor online **grooming**. Onderzoek toont aan dat veel kinderen zonder begeleiding en zonder het hun ouders te vertellen hun online 'vrienden' ontmoeten. Praat hierover met uw kinderen om ervoor te zorgen dat het hen niet overkomt. Communiceren is essentieel.

NETTIQUETTE

Nettiquette verwijst naar goede manieren op het internet en online mensen behandelen zoals u graag behandeld zou willen worden. Kinderen beseffen wellicht niet dat zij online iemand per ongeluk kunnen beledigen. Helaas gebruiken sommige mensen het internet en/of de mobiele telefoon om anderen boos of verdrietig te maken of te treiteren. Dit wordt digitaal pesten genoemd. Een op de vier kinderen kan hiermee te maken krijgen (zie het hoofdstuk Digitaal pesten voor meer informatie).

CHATTAAL

Als jongeren online chatten, gebruiken ze een unieke taal vol **emoticon**s en **acroniem**en! Bekijk onderstaande tabellen om er bekend mee te raken

Indicatieve lijst van chatacroniemen, voor meer informatie zie handige links:

121: one to one

AFK: away from keyboard

A/S/L: age, sex, location (or just „ASL“)

BBB: bye bye baby

B4N: bye for now

BBL: be back later

BF: boyfriend or best friend

BFF: best friends forever

C: see?

Comp: computer

CU: see you

CUL: see you later

CYO: see you online

EGBOK: everything going to be ok

F2F: face to face

G2G or GTG: got to go

JJ: just joking

K: all right /ok

KFY/K4Y: kiss for you

KISS: keep it simple, stupid

KPC: keeping parents clueless

L8R: later

IRL: in real life

LMIRL: let's meet in real life

LOL: laughing out loud, lots of love

LY4E: love you forever

NE1: anyone

NP: no problem/ noisy parents

OIC: oh, I see

OLL: online love

PAL: parents are listening

PAW: parents are watching

<G>: grin

GF: girlfriend

GFN: gone for now

GL: good luck

GM: good morning /good match

HAND: have a nice day

^5: High 5

H2G: have to go

HDOP: help delete online predators

IDK: I don't know

ILU/ILY: I love you / I like you

PIR: parent in room / people in room

PLZ/PLS: please

POS: parent over shoulder

RL: real life

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

TTYL: talk to you later

TY: thank you

WB: welcome back/ write back

WDYT: what do you think

WTGP: want to go private?

WYCM: will you call me?

Emoticons maakt u door leestekens en letters te combineren, zie onderstaande voorbeelden:

Een smiley (met of zonder neus)	**:)** or **: -)** dubbelepunt, (streepje), haakje
Een verdrietig gezichtje (met of zonder neus)	**:(** or **:-(** dubbelepunt, (streepje), haakje
knipogend gezichtje (met of zonder neus)	**;)** or **;-)** puntkomma, streepje, haakje
Verbaasd gezichtje (met of zonder neus)	**: o** or **:-o** dubbelepunt, (streepje), kleine o
Brede lach (met of zonder neus)	**:-D** or **: D** dubbelepunt, (streepje), hoofdletter D
Tong uitsteken (met of zonder neus)	**: p** or **:-p** dubbelepunt, kleine p

HOOFDREGELS

- Neem de tijd om te ontdekken hoe uw kinderen hun tijd online doorbrengen en vraag hun u te laten zien hoe ze met hun vrienden communiceren;

- Leer ze hun privacy online te beschermen door:
  - Veilige profielen aan te maken met ingeschakelde privacy-instellingen
  - Hun wachtwoorden te beschermen
  - Alleen contact te leggen met en berichten te beantwoorden van mensen die ze ook offline kennen
  - Altijd toestemming te vragen aan hun ouders voordat ze foto's van zichzelf, uw gezin, huis, hun school etc. uploaden
  - Persoonlijke informatie, zoals hun telefoonnummer, adres, school, sportteam etc., alleen te delen met mensen die ze in het echt goed kennen

- Zet de thuiscomputer in een gezamenlijke ruimte zodat u toezicht kunt houden op hun online activiteiten;

- Zorg er samen voor dat u:
  - Weet hoe u contactpersonen kunt weigeren of personen kunt blokkeren van een contactpersonenlijst
  - Op de hoogte bent van de veiligheids- en rapportagefuncties die op de door u gebruikte websites zitten

- Kweek vertrouwen door uw kinderen ervan te verzekeren dat ze ook met u kunnen praten over hun fouten, zodat u samen naar een oplossing kunt zoeken! Fouten maken hoort bij het leerproces.

HANDIGE LINKS

Op *http://www.i-respect.nl* staat uitleg over hoe je met elkaar omgaat op internet.

Op *www.chatinfo.nl* staat wat u wel en niet moet doen bij het chatten en wat verschillende chatrooms doen om het chatten zo veilig mogelijk te maken.

Raadpleeg het verslag van Eurobarometer 2007 over Safer Internet for Children:
http://ec.europa.eu/information_society/activities/sip/eurobarometer

3. Digitaal pesten

DIGITAAL PESTEN

Communiceren via het internet en de mobiele telefoon heeft vele geweldige voordelen. Helaas zitten er ook kanten aan die niet zo geweldig zijn: uw kinderen kunnen berichten ontvangen of versturen met inhoud die hun gevoelens of die van anderen kwetst. Het is van belang dat u uw kinderen sociaal aanvaardbaar gedrag aanleert: zelfs onze eigen kinderen zijn geen engeltjes ;-)

Digitaal pesten is het gebruik van nieuwe informatie- en communicatieapparatuur en –diensten om een individu of groep te pesten, te treiteren of te intimideren. Daarvoor kunnen e-mail, chat, instant messaging, mobiele telefoons of andere digitale hulpmiddelen worden gebruikt. In virtuele spelomgevingen kunnen treiteraars de **avatar** van uw kind aanvallen, bijvoorbeeld door die te beschieten, **virtuele bezittingen** te stelen of de avatar te dwingen zich op ongewenste manieren te gedragen.

De meeste problemen die kinderen melden hebben betrekking op het door anderen openbaar maken van persoonlijke informatie op openbare plaatsen. Bijvoorbeeld het posten van een persoonlijke foto of persoonlijke informatie op een openbaar forum. Dergelijk gedrag is onaanvaardbaar, net als **pesten** op school of op de speelplaats. Ouders, docenten en kinderen dienen hier bedacht op te zijn en er direct op te kunnen reageren. In tegenstelling tot bij traditioneel pesten kan een kind bij digitaal pesten hier zelfs mee te maken krijgen als hij/zij niet direct in de buurt van de treiteraars is. De treiteraars kunnen bijvoorbeeld bedreigende berichten naar hun e-mailaccount thuis of hun mobiele telefoon sturen wanneer ze willen, dag en nacht.

Ouders kunnen helpen een omgeving te creëren waar pesten niet wordt getolereerd: leer uw kinderen dat anoniem online zijn niet betekent dat zij zich onverantwoordelijk kunnen gaan gedragen. Ze moeten hun eigen rechten en verantwoordelijkheden kennen en weten hoe ze de rechten van anderen kunnen respecteren.

Zorg altijd voor een open dialoog tussen u en uw kinderen zodat u over eventuele verontrustende situaties kunt praten. Nieuwe technologieën zoals de mobiele telefoon kunnen een uitste-kende aanleiding vormen voor discussie en stof tot nadenken geven!

HOOFDREGELS:

- Voorkom negatieve ervaringen door ervoor te zorgen dat uw kinderen weten hoe ze hun eigen privacy moeten beschermen en dat ze beseffen dat ze de privacy van anderen moeten respecteren;

- Leer uw kinderen om niet te reageren op pestberichten;
- Help uw kinderen te begrijpen door wat voor soort berichten en gedrag anderen zich naar kunnen voelen en hoe ze dit kunnen voorkomen;
- Zorg ervoor dat ze weten hoe ze afzenders van hun contactpersonenlijst kunnen blokkeren;
- Bewaar aanstootgevende berichten, u heeft ze misschien nog nodig als belangrijk bewijs;
- Houd uzelf op de hoogte van de antipeststrategieën op de school van uw kinderen. Werk samen met andere ouders en leerkrachten om pesten en digitaal pesten te voorkomen;
- Houd voeling met de omgeving van uw kinderen; leer hun vrienden, de ouders van hun vrienden, hun docenten en hun klasgenoten kennen;
- Moedig uw kinderen aan om u over eventuele onaangename offline en online ervaringen te vertellen. Verzeker hen ervan dat u voor ze klaarstaat, zelfs als ze onvoorzichtig zijn geweest, en dat u samen met hen oplossingen zult zoeken!
- Zorg ervoor dat uw kinderen begrijpen dat het nooit hun schuld is als ze door iemand worden getreiterd.

HANDIGE LINKS

Op pestweb.nl vindt u gerichte informatie voor ouders, leerlingen en docenten over pesten. Via pestweb kunnen kinderen hun verhaal kwijt en vragen stellen.
http://www.pestweb.nl

Tips voor ouders en kinderen over cyberpesten en gsmpesten vindt u op pestenislaf.nl.
http://www.pestenislaf.nl

De Kindertelefoon is er voor kinderen en jongeren in Nederland en biedt steun door middel van een telefonische en online hulpdienst. De Kindertelefoon is te bereiken op 0800-0432 (gratis) en via *http://www.kindertelefoon.nl.*

Wordt uw kind lastig gevallen in een chatbox? *Op www.chatinfo.nl* leest u wat u kunt doen.

4. Entertainment & Downloaden

HET IS NIET ALLEEN GOUD WAT ER BLINKT OP INTERNET

Het internet is een virtuele ruimte waar zich vele activiteiten afspelen, ook commerciële activiteiten. Als u uw kinderen niet altijd alles geeft waarvoor op tv reclame wordt gemaakt of waar ze in de winkel helemaal van onder de indruk zijn, moet u ze ook leren dat ze ook niet alles moeten willen hebben of geloven waar online voor geadverteerd wordt, bijv. muziek en games, **ringtone**s, andere accessoires en diensten die je online kunt kopen.

Door samen met uw kinderen tijd door te brengen op het internet kunt u ze uitleggen dat producten als ringtones, **wallpaper**s, **mp3**'s, **avatar**s etc. vaak niet gratis zijn. Laat hen als u dergelijke reclame ziet de kleine lettertjes zien om aan te tonen dat ze niet alles op het **net** als vanzelfsprekend moeten aannemen.

Om uzelf te abonneren op een dienst (al dan niet gratis), moet u relevante persoonlijke informatie invullen op een **online formulier**. Vul dergelijke formulieren alleen in als u weet waarvoor uw persoonlijke gegevens worden gebruikt, en weerhoud uw kinderen ervan zulke formulieren in te vullen, tenzij ze die samen met u invullen.

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

ONLINE GAMEN

Online spellen verschillen van andere digitale spellen doordat er een actieve **netwerkverbinding** voor nodig is. Kinderen kunnen games spelen op een cd/dvd op **websites**, **gameconsole**s of mobiele telefoons en andere **draagbare apparatuur**.

Online games variëren van eenvoudige, bekende spellen als Pacman en Tetris tot virtual reality-spellen waarin verscheidene gebruikers samen online spelen en inhoud en verhalen

creëren. Veel van zulke **multiplayer-spel**len ondersteunen virtuele spelersgemeenschappen. Hierdoor kunnen kinderen blootstaan aan risico's die verbonden zijn aan het op het internet ontmoeten van mensen die ze niet kennen (zie het hoofdstuk over Communiceren).

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

Maar niet alle digitale spellen zijn van goede kwaliteit. U moet besluiten welk soort spellen het meest geschikt is voor uw kinderen, en door afspraken te maken, kunt u ervoor zorgen dat de tijd die uw kinderen online doorbrengen met het spelen van het spel niet ten koste gaat van andere activiteiten.

Er bestaat een pan-Europees leeftijdsclassificatiesysteem voor interactieve spellen, **PEGI online**, waar spellen worden geclassificeerd op leeftijd en inhoud. Het systeem wordt ondersteund door diverse fabrikanten, waaronder PlayStation, Xbox en Nintendo, en uitgevers en ontwikkelaars van interactieve spellen in heel Europa. Deze specificaties staan achterop de doos van de spellen die u voor uw kind koopt, maar onthoud: de ene 12-jarige is de andere niet.

De leeftijdsindicatie geeft alleen de schadelijkheid aan, niet de moeilijkheidsgraad. Een 3+ spel is vrij van geweld, discriminatie en seks, maar dat wil niet zeggen dat een kind van 3 het ook kan spelen. Het kan bijvoorbeeld zelfs nog veel te ingewikkeld zijn voor een 8-jarige.

BESTANDEN DELEN & AUTEURSRECHT ©

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

Is het delen van bestanden illegaal?

Het delen van auteursrechtelijke beschermde werken – in de zin van zowel uploaden als downloaden - is niet illegaal als u zelf de maker bent of wanneer de maker toestemming heeft gegeven. Het uploaden van auteursrechtelijk beschermde werken zonder toestemming van de rechthebbende is wel illegaal. Zo lang het voor eigen gebruik is, mogen auteursrechtelijk beschermde werken zoals muziek en films wel van het internet worden binnengehaald (downloaden). Software en games zijn echter van deze regel uitgesloten en het is dan ook illegaal om zonder toestemming van de rechthebbende software en games te downloaden.

Is het delen van bestanden riskant?

Door **bestanden** te **delen** zou u mogelijk gevaar kunnen lopen: er kunnen poorten worden geopend waardoor kwaadaardige programma's en malware uw computer kunnen binnendringen, waardoor de computer niet goed meer kan functioneren. Ook is het mogelijk dat anderen toegang hebben tot uw persoonlijke gegevens of uw computer gebruiken om spam of illegale inhoud te versturen.

HOOFDREGELS

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

KINDEREN & GAMES:

- Maak afspraken met uw kind over de speelduur;
- Laat hen spelen in een gezamenlijke ruimte waar u ze in de gaten kunt houden;
- Houd toezicht op de speelgewoonten van uw kinderen: als u ze op de speelplaats in de gaten houdt, waarom dan ook niet als ze spelen op virtuele plaatsen?
- Bespreek de inhoud van het spel, welke elementen zijn realistisch en welke niet, wat vinden ze leuk?
- Zorg dat u voordat u een spel voor uw kinderen koopt weet dat de inhoud geschikt is voor hun leeftijdscategorie (pan-Europees PEGI-systeem of een nationaal classificatiesysteem).

Als uw kinderen online games met meerdere gebruikers spelen:

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

HANDIGE LINKS

Kom meer te weten over online games en het PEGI-leeftijdsclassificatiesysteem: *http://www.pegionline.eu*

Kijk ook eens op *www.weetwatzegamen.nl* waar u als ouder informatie kunt vinden over games, expertmeningen kunt lezen en ervaringen van ouders met hun gamende kinderen.

Simuze (*www.simuze.nl*) is een Nederlandse muziek community waarbij muzikanten en muziekliefhebbers elkaar ontmoeten en muziek uitwisselen, remixen of verder bewerken. Muzikanten kunnen hun muziek uploaden onder een Creative commons licentie naar eigen keuze. Zo beschermt de muzikant zijn muziek en geeft tegelijkertijd anderen meer vrijheid het te gebruiken.

C. Oplossingen bij de voorgestelde activiteiten

1. Beveiligd en wel

ACTIVITEITEN MET AANTEKENINGEN

Zet de woorden bij de juiste afbeelding: Computerkast (E), muismat (I), beeldscherm (D), luidsprekers (A), webcam (B), printer (C), USB-stick (of geheugenstick) (G), muis (H), CD-Rom (F).

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

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

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

het document door er nogmaals met de rechtermuisknop op te klikken kunt scannen voor het te openen om veilige gewoonten te stimuleren. De meeste anti-virus programma's maken gebruik van de optie om met de rechtermuisknop een document te scannen. In dat geval kunt u bovenstaande teksten volgen. Gebruikt u een ander anti-virus programma, laat uw kind dan zien hoe het documenten kan scannen op virussen op een andere manier.

Volg Hewigs advies op en leer hoe je je **e-mailadres** moet beschrijven als je het echt eens online moet zetten. Zo voorkom je dat je e-mailadres automatisch wordt opgepikt en gebruikt wordt door spammers.
Voorbeeld: cybercat.smith@mymail.com = cybercat punt smith apenstaartje mymail punt com

Beschrijf om te oefenen de e-mailadressen van jullie gezin: *je eigen e-maildres, e-mailadres van jullie gezin, e-mailadres van je moeder, e-mailadres van je vader*

Om te voorkomen dat uw openbare e-mailadres automatisch door software wordt opgepikt voor het verspreiden van spam, kunt u het beschrijven in plaats van het helemaal uit te schrijven. Laat uw kinderen oefenen met de hierboven beschreven techniek. Houd echter in gedachten dat uw kinderen hun e-mailadres niet op het internet moeten zetten, en als ze dat toch doen, ze een e-mailadres moeten gebruiken dat niet hun volledige naam onthult (zie hoofdstuk Communiceren).

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

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

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

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

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

Door interessante sites in de map favorieten (optie in de browserwerkbalk) op te slaan en te ordenen hoeven uw jonge kinderen minder snel informatie te zoeken op het internet.

ALLES OP EEN RIJTJE

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

VOORGESTELDE OPLOSSINGEN BIJ DE SITUATIEKAARTJES

SITUATIE 1. Ga nooit op het internet surfen als je computer niet beveiligd is met bijgewerkte antivirus- en antispywareprogramma's. Dat is net zoiets als een grens zonder grenswachten; je computer kan dan worden geïnfecteerd met schadelijke programma's zoals virussen, Trojaanse paarden, wormen of spyware.

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

SITUATIE 3. Vertrouw als je op het internet naar informatie zoekt niet meteen de eerste goede pagina die je krijgt. Bekijk minstens 3 andere sites en vergelijk de informatie die erop staat. Denk eraan: iedereen met toegang tot het internet kan informatie schrijven en die op het net zetten. Als je een werkstuk of opdracht maakt, moet je altijd de bron vermelden van de informatie en de afbeeldingen die je gebruikt hebt... net als een echte wetenschapper.

2. Communiceren LoL ;-D

ACTIVITEITEN MET AANTEKENINGEN

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

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

Help Zeta een heel goed wachtwoord te maken met behulp van Hewigs tips.

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

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

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

Kijk goed naar deze foto en schrijf op wat je van deze persoon kunt afleiden:

Welke persoonlijke informatie kan worden afgeleid van een foto? Kinderen zijn zich vaak niet bewust van de invloed die afbeeldingen hebben.

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

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

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

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

ONTCIJFER DE CODE: Ontdek wat deze populaire chatacroniemen betekenen.

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

Gebruik toetsencombinaties om deze emoticons uit te beelden: Een smiley – Een verdrietig gezichtje – Knipogend gezichtje – Verbaasd gezichtje – Brede lach – Tong uitsteken

Zie hoofdstuk Communiceren/nettiquette voor meer informatie

ALLES OP EEN RIJTJE

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

VOORGESTELDE OPLOSSINGEN BIJ DE SITUATIEKAARTJES

SITUATIE 4. Als je op het internet bezig bent, kan jouw profiel, of de informatie die je over jezelf geeft, wel tientallen, honderden, duizenden of zelfs miljoenen mensen bereiken. Daarom is het belangrijk om de informatie die je over jezelf geeft zorgvuldig te kiezen. Geef persoonlijke informatie alleen aan mensen die je vertrouwt en/of die je in de offline wereld ook goed kent.

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

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

3. Digitaal pesten

ACTIVITEITEN MET AANTEKENINGEN

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

Uw kinderen mogen hun creativiteit uitleven op het lege vak.

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

Bespreek met uw kinderen welk gedrag zij onaanvaardbaar vinden.

ALLES OP EEN RIJTJE

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

VOORGESTELDE OPLOSSINGEN BIJ DE SITUATIEKAARTJES

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

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

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

4. Entertainment & Downloaden

ACTIVITEITEN MET AANTEKENINGEN

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

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

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

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

ALLES OP EEN RIJTJE

1: (gratis) 2: (formulieren) 3: (val) 4: (kruisje) 5: (negeren) 6: (privacy) 7: raadplegen 8: (download)

VOORGESTELDE OPLOSSINGEN BIJ DE SITUATIEKAARTJES

SITUATIE 10. Online vraaglijsten kunnen een goede manier zijn om als gebruiker je feedback op een website te geven. Wanneer websites echter vragen om je persoonsgegevens, moeten zij het doel daarvan duidelijk aangeven en laten weten waar zij deze gegevens voor zullen gebruiken. Adviseer je kinderen om geen online formulieren in te vullen zonder dat zij de context daarvan begrepen hebben. En dan nog moeten ze altijd voorzichtig blijven met het geven van persoonlijke informatie (zie hoofdstuk Communiceren) .

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

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

D. Glossarium

Aanmelden: zich abonneren op een online-dienst: een nieuwsbrief, discussieforum, e-mail, chatplatform etc. Gewoonlijk moeten gebruikers zich kunnen uitschrijven wanneer ze willen.

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

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

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

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

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

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

geven geïnfecteerd te zijn.

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

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

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

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

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

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

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

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

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

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

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

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

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

Chatten: synchrone communicatie via het internet door middel van geschreven berichten, door

gebruik te maken van chat- en instant messaging-toepassingen (bijv. MSN).

Chatroom: openbare virtuele ruimte voor directe communicatie. Mensen van over de hele wereld kunnen elkaar ontmoeten in chatrooms en met elkaar praten via op het toetsenbord geschreven berichten. Als uw kinderen een chatroom bezoeken, zorg er dan voor dat die geschikt zijn voor hun leeftijd en er toezichthouders en moderators aanwezig zijn.

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

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

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

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

Digitaal pesten: pesten via elektronische media, meestal via instant messaging en e-mail. Het kan bestaan uit herhaaldelijk toegebrachte schade, bedreigingen, seksueel getinte opmerkingen, fysieke aanvallen en kleinerend taalgebruik. Digitale treiteraars kunnen persoonlijke contactinformatie van slachtoffers publiceren en zelfs hun identiteit aannemen om op hun naam materiaal te publiceren met de bedoeling hen te schande of belachelijk te maken.

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

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

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

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

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

Emoticon: een afbeelding, icoontje om gevoelens en emoties over te brengen, bijv. een smiley. Het symbool kan worden gemaakt met gewone toetsenbordtekens en leestekens of met kant-en-klare

tekens van chatrooms, gamerooms, instant messaging-diensten, mobiele telefoons etc.

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

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

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

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

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

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

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

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

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

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

Grooming: het gebruik van chatrooms door pedofielen om kinderen te lokken door zich als leeftijdsgenoten voor te doen. Pedofielen beginnen een gesprek met mogelijke slachtoffers om zo informatie in te winnen over locatie, interesses, hobby's en seksuele ervaringen. Ze gebruiken diverse middelen om kinderen te betrekken bij seksueel getinte gesprekken.

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

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

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

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

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

Illegale inhoud: online-inhoud die volgens nationale wetgeving illegaal is. De meest voorkomende soorten van dergelijke inhoud zijn afbeeldingen van seksueel misbruik van kinderen, illegale activiteit in chatrooms (bijv. grooming) en online-websites die aanzetten tot haat of vreemdelingenhaat.

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

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

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

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

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

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

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

Kraker: iemand die illegaal inbreekt in computersystemen.

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

beeldingen kunnen ook dienen als link naar andere webpagina's.

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

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

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

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

Mobiel: een elektronisch telecommunicatieapparaat, ook wel mobiele telefoon, draagbare telefoon, gsm, smartphone of zaktelefoon genoemd. Het heeft dezelfde basiscapaciteiten als een traditionele vaste telefoonlijn. Tegenwoordig zijn de meeste mobieltjes uitgerust met een camera en hebben vele toegang tot het internet (een rendabele dienst).

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

Net: afkorting voor het internet.

Nettiquette: internetetiquette die beleefdheidsregels voor online-communicatie voorschrijft.

Nickname: synoniem van schermnaam en bijnaam. Het vertegenwoordigt de gebruiker van een online-dienst en wordt beschreven door de gebruiker zelf. Het vertegenwoordigt gebruikers in contactpersonenlijsten, chatrooms etc. Uw nickname, mits goed gekozen, kan uw anonimiteit online beschermen.

Nieuwsgroep: zie definitie forum.

Ouderlijk toezicht: zie definitie gezinsinstellingen.

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

Pesten: pesterij door herhaaldelijk toegebrachte schade, bedreigingen, seksueel getinte opmerkingen, fysieke aanvallen en kleinerend taalgebruik, begaan door een of meer treiteraars.

Poort: een interface op een computer waarmee die kan worden aangesloten op andere apparatuur.

Poorten kunnen intern of extern zijn. Interne poorten maken verbinding met een diskdrive of netwerk, terwijl externe poorten verbinding maken met randapparatuur zoals een printer of toetsenbord.

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

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

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

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

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

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

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

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

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

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

Ringtone: een geluid op een mobiele telefoon voor binnenkomende gesprekken. Er is een grote verscheidenheid aan op maat te maken ringtones en muziek te downloaden en te gebruiken voor eigenaren van een mobiele telefoon, vaak tegen betaling.

Scannen: het met een scanner omzetten van gedrukt materiaal naar digitale bestanden. Door deze

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

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

Schermnaam: zie definitie voor Nickname

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

SIP-Bench: een door de Europese Commissie gesteunde studie waarvoor 30 hulpmiddelen voor toezicht en tegen spam zijn getest op hun doeltreffendheid om kinderen te beschermen tegen schadelijke inhoud op het internet.

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

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

Software: zie definitie voor computerprogramma

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

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

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

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

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

Veiligheidsinstellingen (profiel): een serie van aan uw eigen wensen aan te passen veiligheidsfuncties die gekoppeld zijn aan uw online-profiel (zie definitie). Deze functies hebben meestal betrekking op het openen van afbeeldingen en bestanden, het identificeren van betrouwbare informatieverstrekkers en de mate waarin pornografische inhoud wordt toegestaan.

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

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

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

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

Wallpaper: een patroon, foto of een andere grafische voorstelling die de achtergrond van uw computerscherm vormt.

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

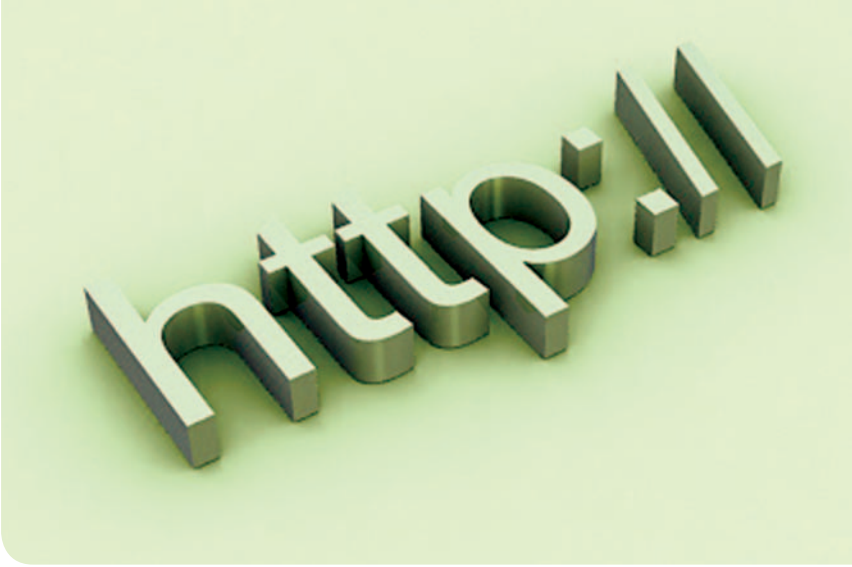
Webcam: een camera die kan uitzenden via het web, in instant messaging, pc-toepassingen voor videoconferenties, chatplatforms etc. Camera's met toegang tot het web bestaan uit een digitale camera die beelden uploadt naar een webserver, ofwel doorlopend, ofwel met regelmatige tussenpozen.

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

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

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

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



E. Nuttige adressen

DIGIBEWUST

Digibewust informeert u over de mogelijkheden maar ook over de gevaren van digitale middelen zoals internet. Op de website vindt u informatie over veilig internetten voor uzelf, uw kinderen en uw bedrijf.
http://www.digibewust.nl

DE HOTLINE

Neem om een rapport te maken over inhoud die u bent tegengekomen op het internet en waarvan u vermoedt dat die illegaal is contact op met het meldpunt:
http://www.meldpunt-kinderporno.nl

KENNISNET

Actuele informatie, handreikingen en links over veilig internetten en computerbeveiliging voor ouders, leraren, kinderen, scholieren is te vinden op:
www.kennisnet.veilig.nl

DE KINDERTELEFOON

is er voor kinderen en jongeren in Nederland en biedt steun door middel van een telefonische en online hulpdienst. De Kindertelefoon is te bereiken op 0800-0432 (gratis) en via *http://www.kindertelefoon.nl*

OUDERS ONLINE

Dit is de grootste ouders-community van Nederland. Voor ouders (en toekomstige ouders) van baby's tot en met pubers.
www.oudersonline.nl

MIJNKINDONLINE

De website 'Mijn kind online' (*www.mijnkindonline.nl*) ondersteunt ouders bij het Internetgebruik door hun kinderen. De site is van de Stichting Mijn Kind Online, een onafhankelijk kenniscentrum Jeugd en Media.

WAARSCHUWINGSDIENST.NL

De waarschuwingsdienst is een bron van informatie over veilig internetten en geeft voorlichting en adviezen over computerbeveiliging. Daarnaast kunt u zich aanmelden voor het ontvangen van waarschuwingen over de nieuwste computervirussen, wormen en beveiligingslekken in software.
http://www.waarschuwingsdienst.nl/

KINDERCONSUMENT

Stichting De Kinderconsument (*www.kinderconsument.nl*) geeft allerlei materiaal uit om kinderen, ouders en leerkrachten te informeren om met allerlei aspecten om te gaan in het commerciële informatietijdperk.

INSAFE

Het Europese netwerk dat het bewustzijn rond e-safety wil vergroten en dat zich richt op het in staat stellen van gebruikers om te profiteren van de positieve aspecten van internetgebruik terwijl potentiële risico's worden vermeden:
http://www.saferinternet.org

ins@fe

DIGI bewust

Gesteund door: upc

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