Guide pour les parents

Protégez vos enfants en ligne!

s@feinternet.be

ins@fe

Soutenu par: telenet

TABLE DES MATIERES

A. Comment utiliser ce kit?

Si vous planifiez pour un an, semez du riz.
Si vous planifiez pour dix ans, plantez des arbres.
Si vous planifiez pour cent ans, éduquez votre enfant.
Proverbe chinois

Cher parent/ éducateur,

Vous tenez en main le kit de sécurité en ligne pour les familles avec des enfants entre 6 et 12 ans. Cette ressource pédagogique a été créée avec la ferme conviction que les nouvelles technologies ne devraient pas séparer les générations mais plutôt les unir. Elle a été réalisée grâce à l'expérience d'Insafe, le réseau paneuropéen de centres de contacts nationaux travaillant à une sensibilisation plus aiguë pour les thèmes de la sécurité sur Internet. La mise au point et la production de ce kit de sécurité en ligne a été soutenue par Telenet.

Tout comme il peut être dangereux de jouer dans une plaine de jeux ou de traverser la route, si l'on ne fait pas attention, l'utilisation d'Internet et des technologies mobiles peut se révéler périlleuse pour les imprudents. Heureusement, il existe des outils permettant de conférer aux utilisateurs d'Internet les connaissances nécessaires sur les avantages et les risques du Web.

Utilisez votre nouveau kit pour soutenir vos enfants dans leur apprentissage d'une utilisation sûre et efficace d'Internet. Le kit offre plus de cinquante conseils de sécurité et exercices pour vous aider à informer vos enfants d'une façon ludique sur la sécurité en ligne, y compris:

- Deux brochures sur la sécurité en ligne: une partie ludique pour toute la famille et un guide pour les parents;
- Les règles d'or;
- Un certificat de famille;
- Des autocollants;
- 12 cartes de situation à découper par les enfants.

Les deux brochures, celle pour la famille et le guide pour les parents, sont marquées avec des couleurs différentes pour souligner les quatre thèmes-clés de la sécurité en ligne: la sécurité, la communication, le divertissement & le téléchargement et le cyber harcèlement. La brochure des parents sert de référence pour la partie ludique: elle contient des informations de fond, des remarques sur les activités et des solutions proposées pour les exercices et les cartes de situation.

La brochure pour la famille est destinée à une utilisation commune par les parents et les enfants. Les quatre thèmes sont abordés à travers l'histoire de deux jeunes, Julien et Céline, leurs parents et le génie de l'informatique Camille. Chaque chapitre contient des activités pédagogiques, y compris des exercices en ligne, des quiz, des règles d'or et des liens utiles.

Lisez l'histoire à voix haute à vos enfants et parcourez ensemble les activités proposées. A la fin de chaque chapitre, vous pouvez utiliser la carte de situation correspondante pour déclencher une discussion avec vos enfants en vue d'améliorer la compréhension du contenu.

Lorsque vos enfants auront parcouru avec succès tout le kit, récompensez-les en établissant un ensemble de règles d'or et en signant ensemble le certificat de famille. En dernier lieu, les enfants peuvent décorer les brochures avec les autocollants.

Vos remarques nous sont très importantes. N'hésitez pas à nous contacter si vous avez des questions ou des commentaires. Nous vous souhaitons beaucoup de plaisir à apprivoiser Internet … en famille!

Surfez en toute sécurité,

INSAFE et saferinternet.be

Ce kit a été soutenue par Telenet.

1. Surfer Safe

UN ORDINATEUR @ LA MAISON

Un ordinateur à la maison peut être une excellente source pédagogique et récréative pour toute la famille. Installez l'ordinateur dans une pièce commune de la maison et établissez des règles spécifiques en ce qui concerne les conditions et la durée d'utilisation de l'ordinateur; ainsi, vous faites déjà un pas important pour assurer la sécurité des jeunes membres de votre famille.

Rappelez-vous que vos enfants peuvent accéder à **Internet** chez des amis, dans des cafés Internet, etc. Voilà pourquoi il est important d'établir un code de conduite qu'ils peuvent appliquer à tout moment et partout.

LA PROTECTION DE VOTRE ORDINATEUR

La sécurité peut être atteinte par une compréhension élémentaire des dangers éventuels et une

connaissance de solutions simples. Ces remèdes incluent des outils technologiques utiles et aussi le bon sens des utilisateurs. Comme tout le reste, le bon sens évolue avec l'âge et la pratique.

Les choses que vous et vos enfants ferez probablement sur votre ordinateur, comme utiliser des **clés USB (clés mémoire)** ou des **CD-ROM**, ouvrir des **pièces jointes** et **télécharger** des **fichiers**, peuvent présenter des menaces. Ces menaces se composent principalement de **programmes informatiques** malicieux **(logiciels malveillants)**, mis au point pour endommager votre ordinateur, voler des données personnelles ou vous envoyer des publicités non désirées.

Des différents types de logiciels malveillants sont présentés aux enfants: des **virus**, des **vers**, des **chevaux de Troie** et des **logiciels espions**. Ils apprennent également à reconnaître les symptômes d'un ordinateur infecté. Ils apprennent à prévenir une infection en n'utilisant Internet que sur des ordinateurs protégés par des programmes antivirus et **anti-espion** mis à jour. On leur conseille également d'être prudent en ouvrant des pièces jointes d'e-mails d'expéditeurs inconnus, en téléchargeant des programmes d'Internet et en utilisant des clés USB ou des CD-ROM.

LA LUTTE CONTRE LE SPAM

80% des e-mails circulant sur Internet sont du **spam** (e-mails non désirés) pouvant facilement influencer vos enfants. La publication par mégarde d'une adresse e-mail sur le **Web** en utilisant un **groupe de nouvelles**, un site de **chat**, un **forum** public, un site de **réseautage social** ou un **forum en ligne** peut produire du spam. Des logiciels spéciaux peuvent recueillir des adresses e-mail du Web pour composer des listes de mailing ; celles-ci sont ensuite utilisées pour distribuer des quantités énormes de spam. Les entreprises recourant à de telles activités sont souvent implantées dans des pays où il n'existe pas de législation pour prévenir des e-mails non désirés!

Les e-mails non désirés (spam) sont souvent liés à la pornographie, aux médicaments, aux transactions financières douteuses, etc. De plus, le spam peut également être la source de programmes malveillants. Dans la plupart des cas, les e-mails non désirés (spam) sont distribués avec des intentions frauduleuses. Voici quelques conseils pour protéger votre famille:

- Utilisez des « **filtres de spam** ». Votre fournisseur d'e-mail propose normalement des options anti-spam que vous pouvez activer dans votre programme e-mail. Contactez votre fournisseur d'e-mail pour de plus amples informations. Vérifiez régulièrement votre **dossier** « **junk** » ou « **spam** » pour vérifier, si des e-mails innocents n'y ont pas atterri. La technologie n'est pas infaillible.
- Apprenez à vos enfants à ne pas ouvrir des e-mails de personnes inconnues. Le spam contient presque toujours des offres et des pièces jointes prometteuses. Montrez-leur comment ils peuvent bloquer l'expéditeur d'un e-mail ou priez-les de supprimer les e-mails suspects.

SURFER SUR LE NET

Même les très jeunes enfants peuvent profiter d'Internet pour s'amuser et pour consulter des **sites Web** pédagogiques. Internet offre néanmoins aussi toutes sortes de contenus qui ne sont pas toujours appropriés à leur âge.

Les moteurs de recherche sont une grande aide pour trouver des contenus sur Internet. Toutefois, comme la recherche dépend du choix des mots-clés, il est facile de tomber sur des contenus non désirés. Un simple mot-clé innocent pourrait mener vers un site Web moins innocent contenant le mot-clé en question. Ci-dessous, vous trouverez quelques conseils pour aider vos enfants à surfer à moindres risques sur Internet :

- Créez un compte d'utilisateur spécial pour votre enfant en utilisant un **système d'exploitation** (Windows, Linux, Mac OS) sur lequel vous pouvez activer les fonctions du **contrôle parental**;
- Examinez les fonctions du contrôle parental de votre **navigateur Internet** et du moteur de recherche. Assurez-vous que vous connaissez les choix offerts par les **paramètres familiaux** de ces outils;
- Proposez des moteurs de recherche adaptés aux enfants, aux jeunes utilisateurs d'Internet dont vous vous occupez;
- Sauvegardez les adresses des sites Web dont vos enfants se servent le plus dans leur dossier de favoris (une option du navigateur). Ainsi, vous pouvez leur permettre d'utiliser leurs endroits favoris du net plusieurs fois sans devoir passer par le moteur de recherche.

Outre l'activation des fonctions de contrôle parental dans votre navigateur et dans le moteur de recherche, vous pouvez utiliser un **filtre** supplémentaire, un logiciel visant à protéger les mineurs des contenus non appropriés sur le Web. Demandez des conseils à votre distributeur ou recherchez des logiciels d'essai sur Internet. Rappelez-vous que rien ne peut remplacer les conseils des parents ou des éducateurs. Les outils techniques ne sont pas infaillibles et peuvent parfois créer un faux sentiment de sécurité, sauf si vous les utilisez en combinaison avec votre bon sens.

Les logiciels de filtrage peuvent être tellement restrictifs qu'ils bloquent des contenus innocents. Ils peuvent par exemple empêcher les enfants de chercher des informations pour un exposé historique sur la Deuxième Guerre mondiale, parce que la recherche mène vers des sites Web décrivant la violence. De plus, chaque filtre, qui peut être enclenché, peut également être déclenché par les jeunes ingénieux souvent experts dans la couverture de leurs traces. Vous ne vous en rendrez compte que si vous apprenez vous-même à utiliser l'ordinateur et les logiciels.

Visitez le site Web de **SIP-Bench**, une enquête soutenue par la Commission européenne ayant testé 30 outils de contrôle parental et d'anti-spam, afin de mesurer leur efficacité dans la protection des enfants entre 6 et 16 ans contre les contenus pernicieux dans les différentes applications d'Internet: la **navigation**, l'e-mail, le **transfert de fichiers**, le chat et les **messages instantanés**.

Outre le fait d'éviter les **contenus pernicieux**, assurez-vous que vos enfants ne croient pas tout ce qu'ils voient ou lisent sur Internet. Dans la partie ludique pour toute la famille, nous suggérons à vos enfants de visiter au moins trois sites Web afin de comparer les contenus. Ils reçoivent également le conseil de mentionner systématiquement la source des informations trouvées à chaque fois qu'ils l'utilisent pour un devoir scolaire.

REGLES D'OR POUR LES PARENTS DES ENFANTS SURFANT SUR INTERNET

- Assurez-vous que votre ordinateur soit protégé par un pare-feu, ainsi que par un logiciel antivirus et anti-espion. Maintenez ces derniers à jour et faites attention aux alertes qu'ils

génèrent. Vérifiez si votre fournisseur d'accès à Internet propose des outils antivirus et anti-espion dont vous pourriez vous servir;

- Utilisez un filtre de spam dans votre programme e-mail et gardez votre adresse e-mail aussi privée que possible en évitant de la publier sur le Web. N'ouvrez pas les e-mails d'expéditeurs inconnus et scannez les pièces jointes avant de les ouvrir;
- Maximisez les options de contrôle parental de vos logiciels : système d'exploitation, navigateur Internet, moteur de recherche et programme d'e-mails. Créez des comptes d'utilisateurs séparés pour vos enfants. Assurez-vous que les paramètres de protection de données soient réglés au niveau le plus élevé (voir le menu « options » dans votre navigateur);
- Envisagez l'utilisation de logiciels de filtrage supplémentaires;
- Contactez votre fournisseur d'accès ou un expert dès que votre ordinateur affiche un comportement bizarre ; il est peut-être infecté. Votre fournisseur devrait également pouvoir vous donner des conseils;
- Si vous ou votre enfant se trouvent confrontés à des contenus pédopornographiques sur internet, vous pouvez en référer à www.stopchildporno.be, en cas de contenus racistes, via www.cyberhate.be;
- Mettez-vous à côté de vos enfants lorsqu'ils sont en train de surfer. C'est une excellente façon d'encourager la discussion et d'augmenter la confiance. Posez-vous le défi d'apprendre ensemble;
- Rappelez-vous que ces règles de sécurité s'appliquent aussi bien à vous qu'à vos enfants. Encouragez-les à vous raconter tout ce qui leur paraît bizarre.

LIENS UTILES

Pour pouvoir surfer sur l'Internet en toute sécurité, l'essentiel est la connaissance: savoir quels sont les risques, savoir comment se protéger et développer ses connaissances. Vous trouverez encore d'avantage d'informations sur le site Internet *www.saferinternet.be*

De l'information actuelle, astuces et liens concernant la sécurité en ligne pour les parents, professeurs, enfants et adolescents sont disponibles sur *www.clicksafe.be*

Voir également *www.spamsquad.be*, le portail belge de la lutte contre le spam.

Si vous trouvez des images pédopornographiques sur Internet, signalez-les sur *www.stopchildporno.be*. Vous pouvez signaler des contenus racistes ou discriminatoires sur *www.cyberhate.be*;

Un point de contact gouvernemental belge sur les abus d'Internet est eCops: *www.ecops.be*

Pour favoriser un Internet plus sûr en offrant des solutions qui protégent les mineurs des mauvais contenus, visitez le site *http://www.sip-bench.org*

2. Communication

LES PIECES DU PUZZLE

Vous rappelez-vous combien il était important pour vous de garder le contact avec vos amis quand vous étiez jeune? Internet fournit une multitude de nouveaux endroits pour rencontrer des amis et propose de nouvelles voies servant à s'exprimer et à garder contact avec ses amis grâce à l'envoi d'e-mails, le partage de fichiers, le blogging et le réseautage social (p.ex. MySpace, Netlog, Facebook, Hi5, Habbohotel) etc. Les adolescents d'aujourd'hui utilisent les nouvelles technologies d'information et communication pour faire des nouvelles expériences et pour se socialiser dans un nouvel espace dont ils croient qu'il est privé et hors portée de la surveillance parentale.

Le chapitre sur la communication initie les parents et les enfants au concept des **données personnelles**, de la **vie privée**, des interactions positives en ligne et de la gestion des risques tels que le contact avec des étrangers. La vie privée est étroitement liée aux concepts des **comptes** & **profils**. Un compte est ce qui rend l'accès possible aux services en ligne.

Hors ligne, un abonnement de bus, une carte de gym ou une carte de membre contiennent des informations personnelles sur vous. Les comptes et les services en ligne sont pareils. Vous ne pouvez pas les utiliser, si vous ne fournissez pas quelques informations personnelles qui forment votre «profil d'utilisateur». Il est important de savoir que vous pouvez choisir les informations personnelles que vous souhaitez rendre accessible et avec qui vous voulez les partager.

Dans la protection de votre vie privée, il s'agit de gérer les informations que vous souhaitez révéler aux autres et non de mentir sur votre personne. Les jeunes sont enthousiastes pour la communication en ligne avec des amis et pour la création de leur image en ligne. Ils ne se rendent toutefois pas toujours compte des conséquences que la publication de leurs données privées peut avoir.

LA CREATION DU PROFIL DE CELINE

Le premier pas dans la protection des informations personnelles est de créer un profil plus sûr en réfléchissant prudemment aux données qu'il reprendra et aux paramètres de protection de la vie privée.

Créez plusieurs comptes e-mail pour les différents contextes en ligne. Par exemple, en utilisant des services en ligne tel que le chat, les messages instantanés, le blogging, etc., incitez votre enfant à utiliser une adresse e-mail neutre et un **nom d'écran (pseudo**). Ainsi, votre enfant n'utilise pas une adresse e-mail révélant son nom entier.

Gardez toujours vos mots de passe secrets. Assurez-vous que vos enfants comprennent qu'ils ne doivent pas partager leurs comptes personnels avec des amis qui peuvent abuser de leur confiance.

Pensez à personnaliser les **paramètres de protection de la vie privée** de votre profil/compte en choisissant l'option privée et non publique. Ainsi, vous avez la possibilité de contrôler qui pourra le voir et avec qui vous pouvez avoir contact. Un profil privé signifie que vous pouvez gérer votre **liste de contacts**. Apprenez à vos enfants à n'accepter le contact qu'avec des personnes qu'ils connaissent déjà hors ligne.

Si vos enfants utilisent des salons de chat, vérifiez:

- s'il y a des vrais modérateurs. L'absence de modérateurs signifie que le chat n'est pas protégé;
- s'il y a des outils permettant d'ignorer ou de bloquer des chatteurs non désirés;
- s'il y a une fonction d'aide ou de signalisation sur le site Web qu'ils peuvent utiliser en cas de problème;
- si les règles de service sont clairement et visiblement stipulées.

PHOTOS ET WEBCAMS

Les enfants doivent comprendre qu'une photo d'eux appartient à leur vie privée et que les images numériques sont extrêmement puissantes. Elles sont faciles à diffuser et à **modifier** et c'est très difficile à les effacer une fois qu'elles ont été envoyées par ordinateur ou par GSM – elles peuvent rester en ligne pour toujours ! Les webcams doivent être utilisées avec prudence et les enfants ne devraient pas les utiliser sans surveillance. Vous et vos enfants ne devriez envoyer vos photos personnelles qu'à des personnes que vous connaissez et auxquelles vous faites confiance – demandez toujours la permission avant de publier une photo de quelqu'un d'autre. Ne laissez pas vos enfants utiliser un ordinateur et une webcam tout seuls dans leur chambre.

LE CONTACT AVEC DES INCONNUS

Les personnes que vous rencontrez en ligne ne sont pas toujours ce qu'elles prétendent être. Apprenez à vos enfants à protéger leur vie privée en ligne, tout comme ils le feraient hors ligne. Vous établissez bien les règles de leur comportement par rapport à des étrangers dans le monde réel, pourquoi ne suivraient-ils pas les mêmes règles sur Internet ?

Vos enfants peuvent établir une relation profonde avec des amis en ligne et ont tendance à faire facilement confiance à des personnes qui se montrent intéressées et compréhensives, même s'ils ne les connaissent pas vraiment. Par conséquent, ils peuvent être tentés de rencontrer ces nouveaux amis hors ligne sans vous en informer. Les enfants ne se rendent souvent pas compte du danger potentiel de telles rencontres et les considèrent peut-être comme insignifiantes. Des études révèlent que beaucoup d'enfants se rendent seuls à des rendez-vous avec des « amis » rencontrés en ligne, sans en informer leurs parents. Parlez-en à vos enfants. Apprenez leurs à toujours fixer un rendez-vous dans un endroit public et à s'y rendre accompagné d'une personne de confiance. La communication est essentielle!!

NETIQUETTE

La **netiquette** concerne les bonnes manières sur Internet et le fait de traiter les autres personnes sur le net de la façon dont on aimerait être traité soi-même. Les enfants ne réalisent peut-être pas qu'ils peuvent par mégarde blesser quelqu'un en ligne. Malheureusement, certaines personnes utilisent Internet et/ou le GSM pour contrarier ou harceler d'autres personnes. Appelé le cyber harcèlement, ce phénomène peut aussi toucher votre enfant (voir le chapitre en question pour de plus amples informations).

LANGAGE DE CHAT

En chattant en ligne, les jeunes utilisent un langage unique plein **d'émoticones** et **d'acronymes**! Jetez un coup d'œil sur le tableau ci-dessous pour vous familiariser avec ce langage

Liste indicative d'acronymes de chat.

@+: à plus tard (à bientôt)

@12C4: à un de ces quatre (à bientôt)

2M1: demain

AMHA: à mon humble service

ATTA : attend

ABS : absent

BJR: bonjour

BIZ, BSX: bise, bisou

BCP: beaucoup

BG: belle ou beau gosse

BB : bye bye

CPG: c'est pas grave

DAC/DAK: d'accord

DSL: désolé

IRL: dans la vie réelle, « in real life »

JMEF: je m'enfous

OUÈ, OÉ: ouais, oui

PI: pas inéressé(e)

PTR: pété de rire

PK: pourquoi

PSK, PQ, PRK : parce que

P-T: peut-être

PTAFQM: pas tout a fait quand même

PV: (en) privé, message privé

QQ1, KK1, QQN: quelqu'un

RAB: rien à battre, rien à dire

RAF: rien à foutre

RAZ: remise à zéro

RGD: rire à gorge déployée

SLT, SLU: salut

SPD: « sois pas dèg »

SPJ: sois pas jaloux

JRE: je reviens

JTA, JDR, JTD: je t'adore

KESTUF: qu'est-ce que tu fais

KOI: quoi

KI: qui

MDP: mot de passe

MDR: mort de rire

(traduction de LoL : laughing out loud)

MPM : même pas mal

NRV: énervé

NN, NAN, NA: non

OSEB: on s'en balance

TFK: tu fais quoi

TG, TAGGLE: ta gueule

TJRS: toujours

TKT: t'inquiète

TLM: tout le monde

TMQ: tu me manques

TSÉ: tu sais

VTFF: va te faire foutre

YX: yeux ou je n'en crois pas mes yeux

2M1: demain

2RI1, DR: de rien

Vous pouvez créer des émoticones en combinant les signes de ponctuation et des lettres. En voici quelques exemples:

Un smiley (avec ou sans nez)	**:)** ou **: -)** Deux points, (tiret), parenthèse
Un visage triste (avec ou sans nez)	**:(** ou **:-(** Deux points, (tiret), parenthèse
Un visage clignotant (avec ou sans nez)	**;)** ou **;-)** Deux points, (tiret), parenthèse
Un visage surpris (avec ou sans nez)	**: o** ou **:-o** Deux points, (tiret), petit o
Un grand sourire (avec ou sans nez)	**:-D** ou **: D** Deux points, (tiret), grand D
Une langue tirée (avec ou sans nez)	**: p** ou **:-p** Deux points, (tiret), petit p

RÈGLES D'OR

- Prenez le temps de découvrir comment vos enfants passent leur temps en ligne et demandez-leur de vous montrer comment ils communiquent avec leurs amis;

- Apprenez-leur à protéger leur vie privée en ligne:

  - en créant des profils sûrs avec des paramètres de sécurité activés;
  - en protégeant leurs mots de passe;
  - en contactant et en ne répondant qu'aux personnes qu'ils connaissent hors ligne;
  - en demandant toujours l'accord des parents avant de télécharger des photos d'eux-mêmes ou de votre famille, de la maison, de leur école, etc.;
  - en ne communiquant des informations personnelles telles que leur numéro de téléphone, leur adresse, leur école, leur équipe de sport etc., qu'à des personnes qu'ils connaissent dans la vie concrète;

- Installez l'ordinateur dans une pièce commune de la famille afin de pouvoir surveiller leurs activités en ligne;

- Ensemble assurez-vous:

  - de savoir comment refuser des contacts ou bloquer des personnes d'une liste de contacts;
  - de connaître les fonctions de sécurité et de signalisation disponibles sur les sites Web que vous utilisez;

- Créez un climat de confiance en assurant à vos enfants qu'ils peuvent vous parler de leurs erreurs pour que vous puissiez trouver des solutions ensemble! Les erreurs font partie de l'apprentissage.

LIENS UTILES

Le site *www.saferinternet.be* vous offre plus d'informations sur la communication intelligente et en toute sécurité et la protection de la sphère privée en ligne. Voir entre autres les ‚Conseils pour cyberkids' et le jeu Spotmonblog. Le jeu prête beaucoup d'attention à l'utilisation de coordonnées personnelles en ligne, choisir un alias, publier des photos... Le jeu est accompagné d'un dossier pédagogique pratique pour des enseignants et des parents.

Sur *www.e-privacy.be*, vous trouverez plus d'informations sur les jeunes et la protection de la vie privée en ligne, entre autres l'étude ‚Cyberkids' e-Privacy', qui a démontré qu'une majorité des sites Internet qui s'adressent à des enfants et à des adolescents collecte des coordonnées de ces jeunes visiteurs sans respecter leur droits à la vie privée.

www.clicksafe.be vous donne plein de trucs et astuces pour déjouer les pièges d'Internet.

Consultez le rapport de l'Eurobaromètre 2007 pour un Internet plus sûr pour les enfants: *http://ec.europa.eu/information_society/activities/sip/eurobarometer*

3. Cyber harcèlement

UN CAS DE CYBER HARCÈLEMENT

La communication par Internet et par GSM a de nombreux avantages. Malheureusement, elle a également certains inconvénients – vos enfants reçoivent ou envoient peut-être des messages avec des contenus qui blessent leurs sentiments ou ceux des autres. Il est important que vous appreniez à vos enfants un comportement socialement acceptable – même nos propres enfants ne sont pas toujours des anges ;-)

Le **Cyber harcèlement**, c'est utiliser les nouveaux appareils et services d'information et de communication pour tyranniser, harceler ou intimider un individu ou un groupe. Les e-mails, le chat, les messages instantanés, le GSM ou d'autres outils numériques peuvent être utilisés. Dans les environnements de jeux virtuels, les tyrans peuvent attaquer l'**avatar** de votre enfant en tirant dessus, en volant des possessions virtuelles ou en forçant l'avatar à se comporter d'une façon non désirée. Quelqu'un peut aussi publier ta photo privée ou des données personnelles sur un forum ou un site Web public.

Comme l'**harcèlement** à l'école ou à la pleine de jeux, un tel comportement est inacceptable; les parents, les éducateurs et les enfants doivent être attentifs et prêts à réagir. Contrairement au harcèlement traditionnel, le cyber harcèlement peut encore toucher l'enfant même s'il n'est déjà plus en présence des tyrans. Par exemple, les tyrans peuvent à tout moment envoyer des messages menaçants aux adresses e-mail à la maison et aux GSM.

Les parents peuvent aider à promouvoir un environnement dans lequel l'harcèlement n'est pas toléré – apprenez à vos enfants que le fait d'être anonyme sur Internet ne leur permet pas d'agir de façon irresponsable. Ils doivent connaître leurs propres droits et responsabilités et savoir comment respecter les droits des autres.

Ayez toujours un dialogue ouvert avec vos enfants pour pouvoir parler de chaque situation inquiétante.

REGLES D'OR

- Prenez des précautions contre les expériences négatives en vous assurant que vos enfants savent comment protéger leur vie privée et respecter la vie privée d'autrui;
- Apprenez à vos enfants à ne pas répondre aux messages harcelants;
- Aidez vos enfants à comprendre quel genre de messages et de comportement pourrait mettre d'autres personnes mal à l'aise et comment les éviter;

- Assurez-vous qu'ils savent comment bloquer des expéditeurs de leur liste de contacts;
- Gardez les messages offensants, ils peuvent vous servir de preuves;
- Informez-vous sur les stratégies anti-harcèlement de l'école de vos enfants. Travaillez ensemble avec d'autres parents et enseignants pour empêcher harcèlement et cyber harcèlement;
- Restez en contact avec l'environnement de vos enfants, rencontrez leurs amis, les parents de leurs amis, leurs enseignants et leurs camarades de classe;
- Encouragez vos enfants à vous raconter tout sur leurs expériences perturbantes hors ligne et en ligne. Rassurez-les, même s'ils font une bêtise, vous serez là pour les aider à trouver une solution!
- Assurez-vous que vos enfants comprennent que ce n'est jamais de leur faute si quelqu'un les harcèle.

LIENS UTILES

Le site *www.saferinternet.be* fournit beaucoup d'explications sur ce qu'est le cyber harcèlement et comment traiter ce phénomène en tant que parent ou enseignant.

www.clicksafe.be propose des fiches adaptées aux parents, professeurs et adolescents. Elles donnent plein d'informations pour prévenir, reconnaître et traiter le cyber harcèlement.

4. Divertissement & Téléchargement

SUR INTERNET, TOUT CE QUI BRILLE N'EST PAS OR

Internet est un espace virtuel proposant une multitude d'activités, y compris des activités commerciales. Si vous ne permettez pas à vos enfants d'avoir tout ce qu'ils voient dans les publicités à la télévision, ou ce qui les impressionne dans les magasins, vous devriez également leur apprendre à ne pas croire ou vouloir tout ce qu'ils voient en ligne, par exemple de la musique, des jeux, des **sonneries** et d'autres accessoires.

Passer du temps avec vos enfants sur Internet vous donne l'occasion de leur expliquer que des produits comme des sonneries, des **fonds d'écran**, des **mp3**, des **avatars** etc. sont rarement gratuits. Lorsque vous trouvez de telles publicités, montrez-leur les petits caractères pour démontrer qu'ils ne doivent pas prendre pour argent comptant tout ce qu'ils trouvent sur le net.

Pour s'abonner à un service (gratuit ou non), vous devez remplir un **formulaire en ligne** avec des informations personnelles importantes. Ne remplissez ces formulaires que si vous savez comment vos données personnelles seront utilisées, et dissuadez vos enfants à remplir de tels formulaires, sauf si vous les remplissez ensemble.

Les **fenêtres pop-up** sont souvent utilisées pour vendre des produits sur Internet. Elles ne sont toutefois pas toujours utilisées à cet effet – cela dépend si elles viennent d'un site Web fiable ou non. En général, si vous faites confiance au site, vous pouvez faire confiance au pop-up. Toutefois, certaines fenêtres pop-up sont utilisées pour lancer des produits peu fiables ou mènent vers des questionnaires en ligne recueillant des données personnelles. Apprenez à vos enfants à fermer les fenêtres pop-up non fiables en cliquant sur la croix rouge dans le coin supérieur droit

JOUER EN LIGNE

Les enfants peuvent jouer à des jeux sur un CD/DVD, sur des sites Web, sur des consoles de jeux ou sur un GSM ou d'autres appareils portables. **Les jeux en ligne** se distinguent des jeux numériques plus anciens parce qu'ils ont besoin d'une **connexion réseau en direct.** Ces jeux en ligne vont de jeux simples et bien connus comme Pacman et Tetris, aux jeux avec une

réalité virtuelle où plusieurs utilisateurs jouent ensemble en ligne en créant des contenus et des histoires. Nombre de ces **jeux multijoueurs** proposent des communautés virtuelles pour les joueurs. On doit donc tenir compte des mêmes règles de sécurité que pour la communication avec des inconnus sur Internet. (voir chapitre sur la communication).

Les jeux jouent un rôle important dans l'évolution d'un enfant, étant donné que les aptitudes sociales et l'esprit stratégique sont développés dans un environnement réglé par des règles de jeux. Nombre de jeux numériques sont attrayants et interactifs et sont utilisés à des buts éducatifs.

Toutefois, les jeux numériques ne sont pas tous de bonne qualité. Vous devez décider quel genre de jeux est le plus approprié pour vos enfants et en établissant des règles, vous pouvez vous assurer que le temps que vos enfants utilisent pour jouer en ligne ne va pas au détriment des autres activités.

Il existe un système de classification paneuropéen pour les jeux interactifs, PEGI online, où des jeux sont classés selon les différents âges et les contenus. Le système est soutenu par plusieurs fabricants, y compris PlayStation, Xbox et Nintendo, ainsi que par des éditeurs et des développeurs de jeux interactifs de par l'Europe. Tenez compte, chaque fois que vous achetez un jeu, de ces pictogrammes que vous trouverez sur le dos de chaque boîte, mais rappelez-vous que tous les enfants de 12 ans ne sont pas tous pareils.

REGLES D'OR

- Encouragez vos enfants à utiliser des sites Web offrant des contenus légitimes, et expliquez-leur que tout ce qui brille n'est pas or sur Internet;
- Expliquez les risques associés au téléchargement imprudent de contenus du net;
- Assurez-vous que votre ordinateur soit protégé et utilisez toujours un programme antivirus mis à jour;
- Lisez toujours la déclaration de confidentialité et les conditions d'utilisateur avant d'installer quelque chose. Vérifiez (sur Internet), si le logiciel du programme que vous souhaitez télécharger est fiable;
- Fermez les fenêtres pop-up non fiables en cliquant sur la croix rouge dans le coin supérieur droit. Ne cliquez jamais à l'intérieur.

ENFANTS & JEUX:

- Etablissez des règles sur la durée de temps pendant laquelle votre enfant peut jouer;
- Mettez l'ordinateur ou la console de jeu dans une pièce commune. Vous pouvez ainsi les tenir à l'œil;
- Surveillez les habitudes de jeux de vos enfants – si vous les surveillez à la plaine de jeux, pourquoi pas lorsqu'ils jouent dans des endroits virtuels?
- Parlez des contenus de jeux et des éléments qui ressemblent à la réalité, ceux qui n'y ressemblent pas et ceux qui les amusent;
- Avant d'acheter un jeu pour votre enfant, assurez-vous que le contenu soit approprié à son âge (système PEGI paneuropéen ou tout autre système de classification national).

Si vos enfants jouent à des jeux en ligne avec plusieurs utilisateurs:

- Choisissez des sites avec des règles strictes et des vrais modérateurs;
- Avisez-les de ne pas révéler leurs données personnelles à d'autres joueurs;
- Recommandez-leur de ne pas rencontrer d'autres joueurs hors ligne, sauf si vous les accompagnez;
- Encouragez vos enfants à signaler l'harcèlement, les menaces ou le langage inacceptable, l'affichage de contenus désagréables ou les invitations à se rencontrer en-dehors du contexte du jeu;
- Retirez votre enfant du jeu ou changez son identité en ligne, si quelque chose dans le jeu ou dans la façon dont il évolue vous met mal à l'aise.

LIENS UTILES

Plus d'infos sur consommer malin, les arnaques sur l'Internet, les objectifs commerciaux de beaucoup de sites pour enfants et adolescents, acheter et publicité en ligne, télécharger, ... sont disponibles sur les sites suivants:

- *www.saferinternet.be*
- *www.crioc.be*
- *www.arnaques.be*
- *www.test-achats.be*
- *http://mineco.fgov.be/*
- *http://www.eccbelgium.be/default_FR.asp*

Jouez aussi le jeu ‚Spotmonblog' sur *www.saferinternet.be*. Le jeu et le dossier pédagogique pour parents et enseignants en annexe t'offrent plus d'informations sur ces aspects de l'Internet. Sur le même site vous trouverez également plus d'infos sur différents aspects des jeux en ligne (e-gaming).

Apprenez-en plus sur les jeux en ligne et le système de classification PEGI:
http://www.pegioline.eu

1. Surfer Safe

COMMENTAIRES SUR LES ACTIVITÉS

Attribue les images aux mots correspondants: la tour de l'ordinateur, le tapis de souris, l'écran, les haut-parleurs, la webcam, l'imprimante, la clé USB (ou clé mémoire), la souris, le CD-Rom.

Un exercice d'échauffement pour familiariser vos enfants avec les différentes parties de l'ordinateur et le reste du matériel hardware. Vous pouvez élargir l'exercice comme bon vous semble.

Demande à tes parents de t'envoyer un e-mail avec une pièce jointe, ou tu t'en envoies un à toi-même. Exerce-toi à effectuer les étapes suivantes: un click droit sur la pièce jointe pour l'enregistrer sur le bureau de ton ordinateur. Va vers le bureau, un click droit sur le document et clique sur scanner. Lorsque tu sais que le document est sûr, tu peux l'ouvrir. Rappelle-toi: click droit et ENREGISTRER – SCANNER – OUVRIR.

Envoyez un e-mail à l'adresse e-mail de vos enfants ou à vous-même en joignant un fichier. Laissez vos enfants suivre les instructions de l'exercice en sauvegardant le document avec un clic droit sans l'ouvrir. Après avoir sauvegardé le fichier sur le bureau ou dans un dossier de l'ordinateur comme «Mes Documents», montrez à vos enfants comment cliquer encore une fois d'un clic droit sur le fichier pour le scanner avant de l'ouvrir. Ainsi, vous les encouragez à prendre des habitudes de sécurité.

Suis le conseil de Camille et apprends à décrire ton adresse e-mail chaque fois que tu dois vraiment la publier en ligne. Tu peux ainsi éviter que ton adresse e-mail ne soit automatiquement captée et utilisée par des spammeurs.

cyberchat.schmid@monmail.com = cyberchat point schmid arrobas monmail point com

Pour t'entraîner, décris les adresses e-mail de ta famille: ton adresse e-mail, l'adresse e-mail de ta famille, l'adresse e-mail de ta mère, l'adresse e-mail de ton père.

Pour éviter que l'adresse e-mail soit automatiquement recueillie par un logiciel dans le but d'envoyer du spam, décrivez-là au lieu de l'écrire. Laissez vos enfants s'entraîner à cette technique comme décrit ci-dessus. Pensez toutefois au fait que vos enfants devraient éviter de publier leur adresse e-mail sur Internet; s'ils le font, ils doivent utiliser une adresse qui ne révèle pas leur vrai nom (voir le chapitre sur la communication).

Pour aider Céline à mieux comprendre avant que Camille ne continue son explication, jette un coup d'œil sur les activités dans ce cadre et entoure celles que tu ne peux faire que lorsque tu es connecté à Internet.

Les très jeunes enfants ne comprendront peut-être pas exactement quelles activités requièrent une connexion réseau. Pour écrire un texte, l'ordinateur ne doit pas être connecté, mais pour chatter il doit l'être. Vous pouvez écouter de la musique sur votre ordinateur en utilisant un CD ou un fichier de musique sauvegardé sur votre ordinateur, mais vous pouvez aussi directement écouter de la musique en ligne. Vos enfants ne doivent indiquer que les activités pour lesquelles une connexion réseau est absolument indispensable.

Avec tes parents, tape www.google.be dans le navigateur. Recherche des informations sur le tyrannosaure et essaye de découvrir quand ce dinosaure a vécu sur terre. Essaie aussi de trouver une bonne image représentant le tyrannosaure. N'oublie pas de vérifier les informations sur trois sites Web différents.

Apprenez à vos enfants de bonnes habitudes de recherche, en leur rappelant de ne pas faire confiance à tout ce qu'ils voient en ligne. Rappelez-leur de chercher et de comparer les informations sur au moins trois sites et de toujours mentionner leurs sources lorsqu'ils écrivent un exposé pour l'école.

Avec tes parents, tape www.google.be dans le navigateur. Recherche des informations sur un certain sujet, par exemple le tyrannosaure, et enregistre les trois sites qui te semblent les plus intéressants en cliquant sur le menu Favoris dans la partie supérieure du navigateur et en les ajoutant à tes sites favoris. Tu peux également créer ton propre dossier.

Sauvegarder et organiser des sites intéressants dans le dossier des favoris (choisir option sur la barre du navigateur) est une bonne façon de réduire le besoin de vos jeunes enfants à rechercher des informations sur Internet.

AS-TU TROUVÉ LA BONNE RÉPONSE?

1: (protégé) 2: (virus), (inconnus), (téléchargeant), (clé mémoire), (infectés), (non protégé) 3: (bizarrement) 4: (connais), (pièces jointes), (titres), (spam) 5: (seule), (spam) 6: (première), (trois), (compare), (chaque personne), (publier) 7: (antivirus), (anti-espions) 8: (parles), (parents) 9: (informe)

SOLUTIONS PROPOSÉES POUR LES CARTES DE SITUATION

SITUATION 1. Ne surfe jamais sur Internet si ton ordinateur n'est pas protégé par un programme antivirus et anti-espion mis à jour. Ce serait comparable à une frontière sans gardes-frontières, ton ordinateur pourrait être infecté par les programmes nuisibles tels que des virus, des chevaux de Troie, des vers ou des logiciels espions.

SITUATION 2. Sois attentif aux e-mails envoyés par des personnes que tu ne connais pas et qui contiennent des pièces jointes ou des e-mails qui promettent 'monts et merveilles' – il s'agit très probablement de spam! Le spam pourrait infecter ton ordinateur avec des programmes nuisibles tels que des virus, des chevaux de Troie, des vers ou des logiciels espions. N'ouvre pas ces e-mails. Bloque l'expéditeur en cliquant d'un clic droit de la souris sur le mail et en sélectionnant «bloquer l'expéditeur» ou supprime-les tout simplement.

SITUATION 3. Si tu cherches des informations sur Internet, ne fais pas confiance à la première bonne page que tu trouves. Visite au moins trois sites différents et compare les informations que tu trouves. Rappelle-toi: tout le monde ayant accès à Internet peut créer et publier des informations sur le net.
Si tu prépares un exposé ou rédiges un devoir, tu dois toujours mentionner la source des informations et des illustrations que tu as utilisées… voilà comment un vrai scientifique procèderait.

2. La communication lol ;-D

COMMENTAIRES SUR LES ACTIVITÉS

Indique à quel point les renseignements suivants sont privés pour toi:
ton numéro de téléphone, ta couleur de cheveux, ton nom, le pays dans lequel tu habites, le nom de ton école, ton adresse, le nom de ton animal domestique, les professions de tes parents, ton adresse e-mail, tes photos, ton âge.

Est-ce que vos enfants ont la même perception de la confidentialité que vous? Les trois couleurs représentent «très privé» (rouge), «assez privé» (orange) et «moins privé» (vert).

Aide Céline à créer un super mot de passe en suivant les conseils de Camille.

Les bons mots de passe contiennent une série aléatoire de différents caractères (chiffres, lettres et signes de ponctuation) et doivent toujours être gardés secrets.

Suis l'exemple de Céline et crée un profil sûr. Crée ensuite un exemple d'un profil dangereux.

Laissez vos enfants créer un profil sûr et ensuite un profil moins sûr révélant des informations privées. Rappelez-leur que la création d'un profil sûr ne les protège pas, s'ils ne continuent pas à protéger leur vie privée en communiquant en ligne.

Analyse cette photo en détail et note ce que tu peux dire de cette personne.

Quelles informations personnelles peuvent être déduites d'une photo? Les enfants ne se rendent souvent pas compte du pouvoir des images.

Suis l'idée de Céline et trouve trois conseils que «Julien, le petit chaperon rouge» pourrait recevoir de Camille pour se protéger contre les «loups du Web».

Vérifiez si vos enfants se rendent compte que le contact avec des étrangers en ligne peut comporter des risques.

Comment aimerais-tu être traité par les gens en ligne? (1….. 2….. 3…..)

Assurez-vous que vos enfants comprennent qu'ils doivent traiter les autres comme ils aimeraient être traités eux-mêmes…

DECHIFFRE LE CODE: Trouve le sens des acronymes de chat les plus populaires en les reliant à leur signification:

Améliorez votre compréhension des acronymes en consultant le chapitre Communication – Netiquette, langage de chat.

Utilise des combinaisons de touches pour représenter les émoticones suivantes: Un smiley - Un visage triste - Un visage clignotant - Un visage surpris - Un grand sourire - Langue tirée.

Voir le chapitre Communication /Netiquette, langage de chat pour plus d'informations.

AS-TU TROUVÉ LA BONNE RÉPONSE?

1: (profil) 2: (vie privée), (responsable) 3: (personnes que tu ne connais pas), (informe) 4:(netiquette), (traité) 5: (émoticone) 6: (mot de passe), (ponctuation) 7: (secret) 8: (refuse) 9: (connais).

SOLUTIONS PROPOSÉES POUR LES CARTES DE SITUATION

SITUATION 4. Lorsque tu utilises Internet, ton profil ou les informations que tu révèles peuvent atteindre des dizaines, des centaines, des milliers et même des millions de personnes. Voilà pourquoi, il faut choisir prudemment les informations que tu veux bien révéler de ta personne. Ne donne des informations personnelles qu'aux personnes auxquelles tu fais confiance et que tu connais déjà bien hors ligne.

SITUATION 5. Michel a probablement donné son mot de passe à son copain qui a décidé de se venger en envoyant des e-mails insultants de sa part. Garde toujours pour toi tes mots de passe, sauf si ça ne te dérange pas, que d'autres personnes lisent tes e-mails ou prétendent être toi pour dire des choses que tu ne dirais pas!

SITUATION 6. Rencontrer un inconnu n'est pas une bonne idée. Mais, si tu penses vraiment pouvoir faire confiance à un ami en ligne qui veut te rencontrer, informe tes parents pour qu'ils puissent t'accompagner. Aucun véritable ami avec de bonnes intentions n'y verra d'inconvénient. Cela posera un problème seulement aux personnes ayant quelque chose à cacher.

3. Cyber harcèlement

COMMENTAIRES SUR LES ACTIVITÉS

Dessine une image de l'invitation que Julien a reçue de ses enseignants. Illustre le logo et le slogan contre l'harcèlement que l'école utilise pour la semaine «anti-harcèlement».

Laissez libre cours à la créativité de vos enfants et laissez-les dessiner dans le cadre vide.

Suis l'exemple de Julien et indique cinq raisons pour lesquelles tu donnerais un «carton rouge» à quelqu'un.

Discutez avec vos enfants des genres de comportement qu'ils trouvent inacceptables.

AS-TU TROUVÉ LA BONNE RÉPONSE?

1: (correctement), (gâchent) 2: (parle) 3: (BONNE) 4: (cyber harcèlement) 5: (bloque) 6: (connais) 7: (répondrais)

SOLUTIONS PROPOSÉES POUR LES CARTES DE SITUATION

SITUATION 7. Ce n'est vraiment pas une façon appropriée d'utiliser ton GSM. Ne transmets pas de messages, d'images ou d'autres documents pouvant blesser un tiers. Traite toujours les autres comme tu aimerais être traité toi-même. Dans une telle situation, parles-en à tes parents ou à un adulte de confiance.

SITUATION 8. Julien doit dire à son ami qu'il n'y peut rien au mauvais comportement du tyran. Il ne doit pas répondre aux messages du tyran, mais les garder comme preuve et les montrer à ses parents ou à ses enseignants. Julien doit également parler avec ses parents qui peuvent l'aider à soutenir son ami.

SITUATION 9. La netiquette indique que tu dois traiter les autres sur le Web comme tu aimerais être traité toi-même. Tu en as certainement appris assez sur ce sujet pour aider Céline.

4. Divertissement & Téléchargement

COMMENTAIRES SUR LES ACTIVITÉS

Ouvre ton moteur de recherche préféré. Tape «sonneries gratuites» ou «jeux gratuits» et jette un coup d'oeil sur les résultats. **Analyse quelques sites Web. Peux-tu détecter des pièges?**

Entraînez-vous en effectuant une recherche avec les mots-clés indiqués et cherchez des pièges de marketing sur les sites Web que vous trouvez. Vous verrez comment l'information en petits caractères est omise des slogans de publicité.

Quel est ton jeu d'ordinateur préféré? Vérifie si tes parents le connaissent et peuvent le décrire. S'ils n'ont aucune idée, explique-le leur d'abord et demande-leur ensuite d'en faire une petite description. Est-ce qu'ils ont réussi? Combien de points leur donnerais-tu sur dix? …/10. Un des parents décrit le jeu préféré de l'enfant. L'enfant dessine une image du jeu.

Savez-vous vraiment à quel genre de jeux vos enfants jouent en ligne et connaissez-vous leur jeu préféré? Laissez-les vous tester!

AS-TU TROUVÉ LA BONNE RÉPONSE?

1: (gratuits) 2: (formulaires) 3: (pièges) 4: (formulaires en ligne) (personelles) 5: (croix) 6: (ignorer) 7: (vie privée) 8: (partager), (toi-même) 9: (demande)

SOLUTIONS PROPOSÉES POUR LES CARTES DE SITUATION

SITUATION 10. Des questionnaires en ligne sont utilisés pour recevoir du feedback des utilisateurs. Si on te demande de donner tes données personnelles, il est important de toujours être au courant du but de cette demande. Apprenez à vos enfants à ne pas remplir des formulaires sauf s'ils connaissent le contexte. Et même si ils le connaissent, ils doivent toujours rester très prudents en ce qui concerne leur vie privée (voir chapitre sur la Communication).

SITUATION 11. Il y a des services gratuits sur Internet, mais les sonneries, les fonds d'écran, les mp3, les avatars et autres sont rarement gratuits. Si Julien regarde de plus près, il découvrira sans doute des petits caractères révélant les frais réels de ces services. Les sonneries, les jeux en ligne, etc. sont tous des excellents moyens de tenter les gens à s'abonner à des services soi-disant 'gratuits' qui leur coûteront en réalité de l'argent.

SITUATION 12. Julien doit se rappeler de garder son identité cachée quand il joue en ligne avec des partenaires qu'il ne connaît pas dans la vie concrète. Il ne doit pas révéler des informations concernant son nom de famille, son adresse et son école, etc. Il doit aussi informer ses parents des jeux auxquels il joue en ligne et ne doit jamais télécharger un jeu d'Internet sans d'abord demander leur permission, parce que leur ordinateur pourrait être endommagé.

D. Glossaire

Abonner: s'enregistrer volontairement à un service ou à un service de nouvelles qui envoie directement des informations à votre boîte de réception personnelle.

Acronyme: une abréviation consistant dans les premières lettres de chaque mot d'une phrase ou d'une expression. Les acronymes sont souvent utilisés par les chatteurs pour communiquer plus rapidement, p.ex. LoL, @+, BIZ (voir le chapitre sur la Communication).

Adresse e-mail: un endroit virtuel vers lequel les messages e-mail peuvent être livrés. Les adresses e-mail se composent de deux parties séparées par le symbole @.

Alerte: une petite boîte apparaît à l'écran pour donner des informations ou vous avertir d'un processus potentiellement nuisible, p.ex. l'arrivée d'un nouveau mail ou l'état de votre protection antivirus.

Anti-espion: un programme qui lutte contre les logiciels espions. Le programme scanne toutes les données entrantes pour détecter les logiciels espions et bloque les menaces trouvées, ou fournit une liste d'entrées suspectes à supprimer.

Antivirus: un programme informatique tentant d'identifier, d'isoler, d'obstruer et d'éliminer les virus informatiques et d'autres logiciels malveillants. L'antivirus scanne d'abord les fichiers pour chercher les virus connus et identifie ensuite les comportements suspects des programmes informatiques qui indiquent une infection.

Auteur: le créateur d'une œuvre littéraire ou audiovisuelle, d'un logiciel, etc. Les droits d'auteur protègent les créations des auteurs contre la reproduction illégale.

Avatar: le profil d'un utilisateur représenté par un nom d'utilisateur et une image, une icone ou

un personnage 3D dans les jeux d'ordinateur en ligne et les mondes virtuels.

Barre d'outils: une série d'icones ou de boutons qui font partie d'une interface du programme d'un logiciel. La barre d'outils sert d'interface en étant toujours disponible et facile à utiliser pour effectuer les fonctions courantes.

Blog: abréviation pour weblog. Un site Web pour lequel un individu ou un groupe génère du contenu, normalement tous les jours, consistant en des textes, des images, des fichiers audio-visuels et des liens.

Blogging: le fait d'écrire ou de mettre à jour votre blog.

CD-ROM: un acronym pour "Compact Disc read-only memory". Il s'agit d'un disque compact non enregistrable avec des données lisibles par un ordinateur. Les CD-ROM sont très populaires pour la distribution de logiciels informatiques.

Chat: communication synchrone par Internet à l'aide de messages écrits en utilisant des applications de chat et de messagerie instantanée (p.ex. MSN).

Cheval de Troie: un code malicieux, un logiciel malveillant qui peut entrer dans votre ordinateur par le biais de procédures semblant inoffensives, comme des jeux ou même des programmes de recherche de virus. Les chevaux de Troie ne se multiplient pas d'eux-mêmes, mais sont normalement créés pour accéder à des données délicates ou pour détruire des données, et peuvent effacer les informations d'un disque dur ou voler des informations confidentielles.

Clé mémoire/USB: appareil de stockage de données pourvu d'un connecteur USB (universal serial bus). Une clé mémoire est normalement petite, légère, amovible et réinscriptible.

Compte: un compte vous permet d'être authentifié et autorisé à utiliser les services en ligne à l'aide d'un nom d'utilisateur et d'un mot de passe. Vous pouvez utiliser votre système d'exploitation pour créer des comptes d'utilisateur séparés pour chaque membre de la famille.

Connexion Internet: fait référence au moyen grâce auquel les utilisateurs se connectent à Internet. Les méthodes courantes de l'accès à Internet incluent la connexion via une ligne téléphonique, des T-Lines, un Wi-Fi, un satellite et des GSM.

Contenu illégal: contenu en ligne qui est illégal et viole la législation nationale. Les contenus les plus courants de ce genre sont des images d'abus sexuels d'enfants, des activités illégales dans les salons de chat, la haine en ligne et les sites Web xénophobes.

Contenus pernicieux: images, textes, documents, etc. dont le contenu peut causer des dommages, p.ex. des images illustrant de la violence sont inappropriées et pernicieuses pour les enfants et les adolescents.

Contrôle parental: voir définition pour les paramètres de famille.

Cookies: un fichier placé dans votre navigateur par un site Web. Chaque fois que vous accédez à nouveau au site Web, le cookie est renvoyé au serveur sur lequel le site Web est stocké. Les cookies témoignent de vos préférences de sites et sont utilisés par des établissements de vente en ligne. Le rejet de cookies peut rendre certains sites Web inutilisables.

Corbeille: un répertoire informatique dans lequel des fichiers supprimés sont temporairement stockés avant que les utilisateurs ne les suppriment définitivement. Vous devez régulièrement

supprimer les vieilles données non désirées de la corbeille pour libérer de la place sur le disque dur, la mémoire interne de votre ordinateur.

Cracker (n.m): une personne qui accède illégalement à des systèmes informatiques.

Cracker (v): copier illégalement des logiciels commerciaux en violant les droits d'auteur.

Cyber harcèlement: fait référence à l'harcèlement par les medias électroniques, normalement par l'envoi de messages instantanés et d'e-mails. Elle peut inclure des attaques, des menaces, des remarques sexuelles et des paroles péjoratives. Les cybertyrans publient par exemple des informations personnelles des victimes, et assument même leur identité pour publier du matériel à leur nom dans l'objectif de les diffamer ou de les ridiculiser.

Données personnelles: toute information pouvant être liée à une personne. Si des données personnelles doivent être recueillies, traitées et stockées, les raisons doivent être explicitement déclarées.

Dossier: une entité dans un système de fichiers qui contient un groupe de fichiers et/ou d'autres répertoires. Les dossiers peuvent contenir une multitude de documents et sont utilisés pour organiser les informations.

Dossier junk/spam: dans une boîte e-mail, l'endroit où les mails considérés comme spam ou junk sont stockés.

Droits d'auteur: une série de droits exclusifs réglant l'utilisation d'une idée, d'un travail ou d'information. Les droits d'auteur sont représentés par le symbole «©».

E-mails: un moyen de communication écrite et électronique qui vous permet d'envoyer des messages avec tout genre de fichier informatique en pièce jointe – texte, images, audio et autres.

Emoticone: une image - une icone - utilisée pour exprimer des sentiments et des émotions, p.ex un smiley. Elle peut être symbolisée en utilisant des caractères standards de clavier et des signes de ponctuation, ou en utilisant des caractères préétablis et proposés par les salons de chat, les salons de jeux, les services de messagerie instantanée, les GSM, etc.

Favoris: un fichier du navigateur à personnaliser pour sauvegarder les liens/signets. Les signets peuvent être organisés dans des sous-dossiers et/ou marqués par un mot-clé pour faciliter la recherche.

Fenêtre pop-up: une fenêtre qui apparaît soudain lors d'une visite sur un site Web ou en appuyant sur une touche spéciale. D'habitude, la fenêtre pop-up contient un menu d'options et reste sur l'écran jusqu'à ce qu'on sélectionne l'une des options ou la ferme en cliquant sur la croix dans le coin droit supérieur.

Fichier informatique: une archive/une collection d'informations liées (documents, programmes, etc.) enregistrées sur un ordinateur sous son propre nom de fichier. Les fichiers d'ordinateur peuvent être considérés comme l'homologue moderne des documents papier qui étaient conservés dans les dossiers de bureau et les bibliothèques.

Filtre: application réglant l'accès aux informations ou aux services spécifiques d'Internet, vous avertissant des sites Web problématiques, retenant la navigation de l'utilisateur, bloquant les sites Web à risques et pouvant même éteindre l'ordinateur. Les systèmes de filtrage sont installés sur des ordinateurs individuels, des serveurs, des téléphones avec accès à Internet, etc.

Filtre de spam: une application bloquant les messages de spam de façon à ce qu'ils n'arrivent pas dans votre boîte de réception.

Flaming: une interaction hostile et insultante entre des utilisateurs d'Internet. Ceci a normalement lieu dans des forums de discussion, dans la discussion relayée par Internet (Internet Relay Chat – IRC) ou même par e-mail.

Fond d'écran: un dessin, ou une image, ou une autre représentation graphique qui forme l'arrière-plan de votre écran d'ordinateur.

Formulaire (formulaire en ligne): un document formaté contenant des champs vides pour vous permettre d'y entrer des données. La forme électronique peut être remplie avec des textes libres ou en choisissant des alternatives dans des listes préétablies (liste déroulante). Après l'envoi, les données sont directement envoyées à une application de traitement qui entre les informations dans une base de données.

Forum: un groupe de discussion en ligne où les participants aux intérêts communs peuvent ouvertement échanger des messages sur des sujets différents.

Groupe de nouvelles: voir définition du forum.

Hacker: terme populaire pour designer une personne qui s'adonne au cracking informatique (voir «cracker»). Est parfois utilisé dans des cercles informatiques pour désigner une personne enthousiasmée par les ordinateurs.

Harcèlement: attaques, menaces, remarques sexuelles, paroles péjoratives et assauts physiques perpétrés par un ou plusieurs tyrans.

Inscription: l'abonnement à un service en ligne: newsletter, forum de discussion, e-mail, plateforme de chat, etc. Normalement, les utilisateurs devraient avoir la possibilité de se désinscrire à tout moment.

Internet: un réseau mondial de réseaux d'ordinateurs interconnectés publiquement accessible permettant la transmission et l'échange de données. Il comprend des réseaux académiques, commerciaux et gouvernementaux ainsi que des réseaux domestiques plus petits proposant de nombreux services tels que l'information, les e-mails, le chat en ligne, le transfert de fichiers, etc.

Jeux en ligne massivement multijoueurs: des jeux offrant un vaste monde 3D, peuplé de milliers de joueurs assumant des rôles à caractères fictifs et se faisant concurrence. Les jeux de rôles, où les participants créent ou suivent ensemble une histoire, dominent dans cette catégorie.

Jeu numérique: un jeu créé par des développeurs de jeux et joué sur un ordinateur. Un jeu en ligne est défini comme étant un jeu numérique nécessitant une connexion réseau directe pour pouvoir être joué. Les jeux en ligne peuvent soutenir l'interaction entre une multitude de joueurs.

Junk mail: messages e-mail non désirés, quasi identiques qui sont envoyés aux adresses e-mail de gens. Étant donné qu'Internet est public, le junk mail et le spam sont difficiles à éviter.

Lien: une référence vers un document disponible en ligne (page web, document écrit, image, etc). Lorsque vous cliquez sur le lien, vous êtes dirigé vers une nouvelle page ou un autre site Web. Les liens écrits sont normalement bleus et soulignés, mais ils peuvent également

être d'une autre couleur et non soulignés. Des images peuvent également servir de liens vers d'autres pages Web.

Logiciel: voir définition du programme informatique.

Logiciel d'essai: un logiciel que vous pouvez essayer avant de l'acheter. Les versions d'essai de logiciels contiennent normalement toutes les fonctions de la version normale, mais ne peuvent être utilisées que pendant une période limitée.

Logiciel espion: des logiciels malveillants secrètement attachés à des fichiers téléchargés d'Internet qui s'installent d'eux-mêmes sur le PC et surveillent les activités. Ils envoient des informations à un tiers, souvent des entreprises tâchant d'établir des profils personnels pour envoyer des publicités ou d'autres informations, ou des crackers qui souhaitent accéder à des données privées.

Logiciel gratuit et logiciel partagé: en général, les logiciels sont protégés par les droits d'auteur et ne peuvent donc pas être téléchargés. Un logiciel gratuit est un logiciel dont le détenteur des droits d'auteur accepte que le logiciel soit utilisé gratuitement par tout le monde. Un logiciel partagé est un logiciel dont le détenteur des droits d'auteur accepte que le logiciel soit utilisé par tout le monde pendant une période d'essai. Après cette période, l'utilisateur doit payer une redevance pour continuer à utiliser ce service.

Liste de contacts: une collection de contacts dans un programme de messagerie instantanée et d'e-mail, dans les jeux en ligne, sur les GSM, etc. Des contacts peuvent être ajoutés, refusés ou supprimés.

Matériel hardware: la partie physique d'un ordinateur, contrairement au logiciel d'un ordinateur, qui agit au sein du matériel hardware. Le hardware peut se trouver à l'intérieur: cartes mères, disques durs et mémoire vive (RAM) – souvent désignés comme composantes; ou à l'extérieur: écrans, claviers, imprimantes, etc. – aussi appelés périphériques.

Malware: l'abréviation anglaise pour logiciel malveillant, c'est-à-dire des logiciels créés dans le but de s'infiltrer ou d'endommager un système informatique sans l'accord du propriétaire. En font partie les virus informatiques, les vers, les chevaux de Troie, les logiciels espions, les logiciels gratuits malhonnêtes (publiciels) et d'autres logiciels malveillants et non désirés.

Messagerie instantanée (MI): une forme de communication instantanée et simultanée entre deux utilisateurs ou plus. MI vous permet de communiquer avec une liste sélectionnée de contacts. Lorsque les personnes dans votre liste de contacts sont en ligne, vous êtes immédiatement avertis.

Mobile: un appareil de télécommunication électronique, aussi connu comme téléphone portable, téléphone cellulaire, GSM, smartphone. Il dispose des mêmes fonctions de base qu'un téléphone fixe normal. Aujourd'hui, la plupart des téléphones portables disposent d'un appareil photo et un bon nombre propose l'accès à Internet (service payant).

Modifier: le processus de modification d'une image, d'un fichier, d'une photo ou d'une illustration d'une façon apparente ou non apparente. De nos jours, il existe un grand nombre d'outils pouvant être utilisés pour influencer le contenu ou la forme de données pour créer un résultat ne correspondant pas à la réalité.

Mot de passe: une série de caractères secrets permettant à son propriétaire d'accéder à un fichier, à un ordinateur, à un compte ou à un programme; il s'agit d'une mesure de sécurité

contre les utilisateurs non autorisés (voir chapitre sur la communication).

Moteur de recherche un outil utilisé pour chercher des informations contenues sur un site Web. Les plus connus sont Google et MSN Search. Des moteurs de recherche disposent de préférences d'utilisateurs avancées qui peuvent inclure des paramètres de sécurité intéressants.

Mp3: un format de codage spécifiquement audio. La taille d'un fichier mp3 est un dixième du fichier audio original, mais le son a presque la qualité d'un CD. En raison de leur taille réduite et de la haute fidélité, les fichiers mp3 sont devenus populaires pour sauvegarder des fichiers de musique sur les ordinateurs et les appareils portables.

Navigateur: un programme utilisé pour visualiser des sites Web. Internet Explorer, Netscape Navigator et Firefox sont trois des navigateurs les plus utilisés pour Windows, Safari est fréquemment utilisé sur les Mac. La plupart des versions récentes des navigateurs offrent des options de contrôle parental.

Naviguer: le fait d'utiliser le navigateur pour visualiser des sites Web ou surfer sur le net.

Net: abréviation pour Internet.

Netiquette: étiquette d'Internet qui établit les règles de politesse pour les communautés en ligne.

Nom d'écran ou pseudo: voir définition du surnom.

Page d'accueil: il s'agit de la page Web qui se charge automatiquement lorsque le navigateur démarre. Le terme est également utilisé pour désigner la première page ou la page principale d'un site Web (voir définition).

Paramètres de famille: aussi appelés contrôle parental. Les paramètres utilisés pour personnaliser un navigateur ou un autre outil du Web, en vue de le rendre plus adapté aux enfants par l'utilisation d'options telles que le filtrage du contenu, la limitation du temps, le contrôle des jeux, etc.

Paramètres de protection des données: une série de détails privés spécifiques au compte que vous pouvez éditer de façon à augmenter la protection des données contre la révélation d'informations personnelles, les cookies, etc.

Paramètres de sécurité (profil): une série d'options de sécurité à personnaliser qui est liée à votre profil en ligne (voir définition). D'habitude, ces options sont liées à l'ouverture d'images et de fichiers, à l'identification de fournisseurs d'information de confiance et au niveau de permission pour les contenus adultes.

Pare-feu: une partie du matériel hardware (intégré dans votre routeur) ou un logiciel (installé sur votre ordinateur) configuré en vue d'empêcher les utilisateurs non autorisés (hackers et crackers) à accéder à l'ordinateur ou à un réseau d'ordinateurs connectés à Internet.

Partage de fichiers: échange en ligne de fichiers entre des utilisateurs d'ordinateur. Le terme couvre aussi bien le fait d'offrir des fichiers à d'autres utilisateurs (télécharger en amont) que celui de copier des fichiers d'Internet vers un ordinateur (télécharger en aval). Les fichiers sont normalement partagés à travers des réseaux P2P (peer-to-peer).

Pièce jointe: un fichier informatique qui est envoyé en même temps qu'un message e-mail. Les vers et les virus sont souvent distribués sous forme de pièces jointes aux e-mails. Les e-mails

avec pièces jointes provenant d'expéditeurs inconnus sont à considérer comme suspects.

Possession virtuelle: une série d'objets que chaque joueur d'un jeu reçoit. Chaque joueur possède ses objets virtuellement par un terminal informatique montrant les objets.

Pornographie enfantine: la pornographie enfantine a des définitions légales différentes dans les différents pays. Au minimum, la pornographie enfantine est définie comme étant une image montrant une personne - un enfant – se livrant à des activités explicitement sexuelles ou étant représentée de façon à donner cette impression.

Port: une interface sur un ordinateur utilisé pour le connecter à un autre appareil. Les ports peuvent être internes ou externes. Les ports internes établissent une connexion avec un lecteur de disque ou un réseau, tandis que les ports externes se connectent à un appareil périphérique comme une imprimante ou un clavier.

Privé: informations sur un individu ou un groupe qui ne sont pas révélées au public. Quand quelque chose est privé pour quelqu'un, c'est généralement considéré comme étant personnel.

Processeur: ou unité centrale de traitement (Central Processing Unit - CPU) est la partie d'un ordinateur qui traite les données, génère les signes de contrôles et stocke les résultats. Avec la mémoire de l'ordinateur, elle forme la partie centrale de l'ordinateur.

Profil: informations personnelles des utilisateurs se trouvant sur des sites de réseautage social, des systèmes de messagerie instantanée, des applications de chat en ligne, des jeux en ligne, etc. Les profils peuvent être publics ou privés et sont personnalisés par les utilisateurs pour représenter leur personne dans des environnements virtuels.

Profil d'utilisateur: une série d'informations décrivant un utilisateur spécifique d'un logiciel, d'un site Web ou un autre outil technique. Typiquement, il inclut des informations telles que le nom d'utilisateur, le mot de passe et d'autres détails (p.ex. la date de naissance, les intérêts).

Programme informatique: normalement appelé logiciel. Le logiciel se compose d'une séquence structurée d'instructions écrites par des programmateurs informatiques permettant à l'ordinateur d'effectuer des tâches. Lorsque vous achetez un logiciel, il se trouve souvent sur un CD-ROM (voir définition), un moyen physique pour stocker les programmes.

Protection des données: la possibilité pour un individu ou un groupe de contrôler le flux d'information sur leur personne et de ne se révéler que sélectivement. La protection des données est parfois liée à l'anonymat, le souhait de passer inaperçu dans le monde public.

Répertoire: une unité d'organisation que votre ordinateur utilise pour organiser les dossiers et les fichiers dans une structure hiérarchique, p.ex. Mes Documents, Mes images, etc.

Réseau P2P: un réseau peer-to-peer (P2P) permet à ceux qui y sont connectés d'échanger des fichiers par le téléchargement en amont et en aval (voir définition). Il ne s'agit que d'une des façons de partager des fichiers sur Internet. Certains services de partage de fichiers sont illégaux.

Réseautage social: des communautés de membres en ligne partageant des intérêts et des activités, et qui se contactent et se fréquentent en ligne en utilisant des logiciels et des services appropriés (voir sites de réseautage social).

Salon de chat: endroit public virtuel pour la communication en temps réel. Des personnes

de par le monde entier peuvent se rencontrer dans les salons de chat et discuter à l'aide de messages qu'ils tapent sur leur clavier. Si vos enfants utilisent des salons de chat, assurez-vous qu'ils soient adaptés à leur âge et qu'il y ait des surveillants et des modérateurs.

Scanner: l'action ou le processus de convertir du matériel imprimé en fichier numérique en utilisant un scanner. Cette conversion vous permet de les visualiser sous forme de fichiers électroniques sur votre ordinateur et de les distribuer en ligne.

Second Life: une communauté 3D, bien connue sur le Web, mise à disposition par une entreprise implantée aux Etats-Unis, Linden Labs. Les utilisateurs peuvent se contacter virtuellement à l'aide d'un avatar (voir définition), créer des maisons et de nombreux environnements, échanger et gagner de l'argent virtuel, etc.

Service d'assistance: un service par e-mail et parfois par téléphone. Les enfants peuvent y formuler leurs soucis sur des contenus illégaux et pernicieux ou des expériences désagréables ou effrayantes relatives à leur utilisation des technologies en ligne.

Service d'assistance téléphonique: un service d'assistance téléphonique ou un service basé sur le Web qui permet de signaler des contenus supposés illégaux et/ou une utilisation illégale d'Internet. Les services d'assistance téléphoniques sont tenus à mettre en place des procédures transparentes et efficaces pour traiter les plaintes et s'assurer du soutien du gouvernement, de l'industrie, des agences du maintien de l'ordre et des utilisateurs d'Internet dans les pays concernés.

Signaler: une fonction qui permet aux utilisateurs d'endroits virtuels publics de signaler un problème (technique, comportement inacceptable d'un utilisateur, contenu illégal, etc.) à un modérateur ou au webmaster.

SIP-Bench: une enquête soutenue par la Commission européenne ayant testée 30 outils de contrôles et d'anti-spam, afin d'évaluer leur efficacité dans la protection des enfants contre les contenus pernicieux sur Internet.

Site Web: un emplacement sur le World Wide Web. Chaque site Web contient une page d'accueil, le premier document que l'on voit en entrant sur le site. Les sites contiennent normalement des liens vers d'autres fichiers et sites. Les sites Web appartiennent à des individus, des entreprises ou des organisations et sont gérés par ceux-ci.

Sites de réseautage social: des plates-formes virtuelles abritant des communautés de membres partageant les mêmes intérêts et activités. Les membres doivent créer des profils d'utilisateur et peuvent partager des outils pour télécharger des textes, des images ou d'autres fichiers, publier des messages et participer à des forums. De nombreux sites de réseautage social sont interdits aux enfants de moins de 13 ans et offrent des paramètres de sécurité pour les profils.

Sonnerie: son d'un téléphone portable pour les appels entrants. Une grande variété de sons et de musique à personnaliser est disponible pour les propriétaires de GSM; ils peuvent les télécharger, souvent contre paiement, et les utiliser.

Surnom: synonyme du nom d'écran ou pseudonyme. Il représente l'utilisateur d'un service en ligne et est choisi par l'utilisateur lui-même. Il représente les utilisateurs dans les listes de contacts, les salons de chat, etc. Les surnoms peuvent protéger votre anonymat en ligne s'ils sont bien choisis.

Spam: e-mail non désiré, normalement de nature commerciale, envoyé en masse. L'envoi de

spam à d'autres personnes est certainement l'une des violations les plus célèbres d'Internet.

Système d'exploitation: un programme faisant fonctionner les fonctions de base d'un ordinateur et permettant à d'autres programmes de tourner. Des exemples bien connus sont Windows, Linux et Mac OS.

Téléchargement: fait référence au processus de copier un fichier d'un service en ligne vers un ordinateur.

Transfert de fichiers: le fait de transmettre des fichiers par un réseau informatique. Du point de vue de l'utilisateur, le transfert de fichiers est souvent désigné comme téléchargement en amont ou en aval.

URL (Uniform Resource Locator - localisateur uniforme de ressource): l'adresse d'un site Web ou d'un fichier spécifique sur Internet. Elle ne contient pas de caractères spéciaux ou d'espaces et utilise des barres obliques pour dénoter les différents répertoires. La première partie de l'adresse indique le protocole à utiliser, la deuxième partie spécifie l'adresse IP ou le nom du domaine où la ressource se trouve.

Vers: un type spécial de virus qui se renouvelle de lui-même et peut se propager sans l'intervention du propriétaire de l'ordinateur vers un grand nombre d'ordinateurs; il peut endommager un réseau, consommer des largeurs de bandes énormes, éteindre un ordinateur, etc.

Virus: un type de code malicieux, un logiciel malveillant créé pour se propager à l'aide de l'intervention des utilisateurs. D'habitude, il se propage par des pièces jointes aux e-mails, mais également par des outils de mémoires externes infectés (clé USB, CD-ROM).

Voix sur réseau IP (VoIP): une technologie permettant aux utilisateurs de parler par Internet, souvent après avoir téléchargé un logiciel client. Les appels sont gratuits pour les utilisateurs qui s'appellent avec le même logiciel client VoIP (p.ex. Skype, Voicebuster). De tels logiciels offrent normalement aussi des possibilités de chat et de partage de fichiers.

Vol d'identité: le vol d'informations personnelles (p.ex. nom, date de naissance, numéro de carte de crédit) et le fait de les utiliser illégalement.

Web: abbreviation pour World Wide Web. Une collection de documents en ligne formatés en HTML (HyperText Markup Language) qui contient des liens vers d'autres documents, des graphiques, des fichiers audio et vidéo. Le web est une partie d'Internet.

Webcam: une caméra qui peut diffuser à travers le Web, dans un système de messagerie instantanée, des applications de conférence vidéo sur ordinateur, des plates-formes de chat, etc. Les caméras avec accès au Web incluent une caméra numérique qui télécharge des images vers un serveur du Web, soit en continu ou à des intervalles régulières.

E. Adresses utiles

SAFERINTERNET.BE

Saferinternet.be est une collaboration entre Child Focus et le CRIOC. Le projet et ce site font de la promotion pour une utilisation sûre et sage de l'Internet et des TIC. Ce projet Safer Internet belge fait partie du programme Safer Internet Plus de la Commission Européenne. Sur www.saferinternet.be, vous trouverez toutes les infos sur les risques liés aux technologies en ligne: fiches thématiques, dossiers, points de vue, fiches pédagogiques, jeux, films, liens intéressants, etcetera.

WWW.WEB4ME.BE

Tu rencontres un problème sur l'Internet? Alors, web4me est l'adresse qu'il te faut! Ce site Internet est destiné à des jeunes, mais offre également de l'information utile pour parents et enseignants: comment réagir à des problèmes? Comment les éviter? Où trouver du recours?

WWW.CLICKSAFE.BE

www.clicksafe.be est un site Web de Child Focus qui donne plein d'informations concer-

nant la sécurité en ligne aux enfants, adolescents, parents et professeurs.

Points de contact belges:

- *www.stopchildporno.be*: point de contact civil pour signaler les images d'enfants abusés sexuellement, trouvées par hasard sur Internet.
- *www.cyberhate.be*: point de contact civil pour les contenus discriminatoires ou racistes sur Internet.
- *www.ecops.be*: point de contact du Federal Computer Crime Unit de la Police fédérale sur lequel vous pouvez signaler toute forme de criminalité constaté sur Internet.

INSAFE

Le réseau européen de sensibilisation pour l'e-sécurité vise à aider les utilisateurs à bénéficier des aspects positifs d'Internet tout en évitant les risques potentiels:
http://www.saferinternet.org

s@ferinternet.be

ins@fe

Soutenu par: telenet

Titre: Kit de sécurité en ligne pour toute la famille • Créé par Insafe/Liberty Global-UPC en 2008
Préfixe: 9789078209 • Id 51950 • NUMERO ISBN: 9789078209577 • EAN: 9789078209577