Directives pour la protection de l'enfance en ligne, destinées aux enfants

www.itu.int/cop

REMERCIEMENTS

Les présentes directives ont été préparées par l'Union internationale des télécommunications (UIT) et une équipe d'auteurs issus de grandes institutions actives dans le secteur des technologies de l'information et de la communication (TIC) et de la sécurité des enfants sur Internet. Elles n'auraient pas vu le jour sans le temps, l'enthousiasme et le dévouement des auteurs qui y ont contribué.

L'UIT exprime sa reconnaissance aux auteurs ci-après (liste dans l'ordre alphabétique), pour avoir consacré leur temps à ce projet et y avoir contribué par leurs précieux éclairages:

- Cristina Bueti (ITU)
- Maria José Cantarino de Frías (Telefónica)
- John Carr (Children's Charities' Coalition on Internet Safety)
- Dieter Carstensen, Cristiana de Paoli and Mari Laiho (Save the Children)
- Michael Moran (Interpol)
- Janice Richardson (Insafe)

Les auteurs adressent tous leurs remerciements à Kirstin Kvigne (Interpol) pour sa révision et ses commentaires détaillés.

L'UIT tient à témoigner sa gratitude à Salma Abbasi de eWWG pour son précieux engagement dans l'initiative pour la Protection de l'enfance en ligne (COP).

Des informations et des documents supplémentaires en rapport avec le présent projet de directives figurent à l'adresse: http://www.itu.int/cop/ et seront régulièrement actualisés.

Les lecteurs qui auraient des commentaires à faire ou des informations supplémentaires à fournir sont invités à contacter Mme Cristina Bueti à cop@itu.int

Table des matières

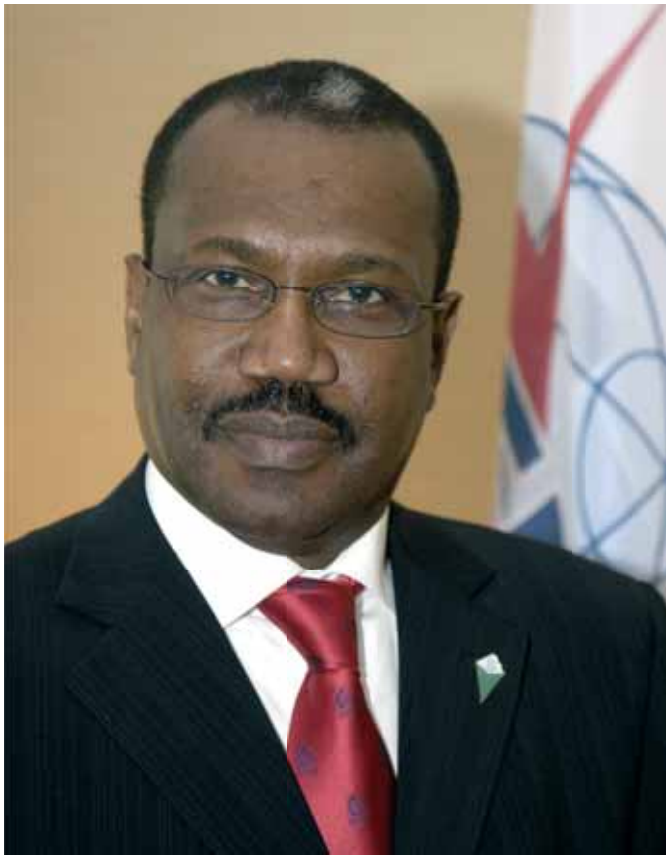
mmm

La Convention des Nations Unies sur les droits de l'enfant définit comme enfant toute personne de moins de 18 ans. Les présentes directives abordent des questions qui touchent les personnes de moins de 18 ans dans le monde entier. Néanmoins, il est très peu probable qu'un internaute de 7 ans ait les mêmes besoins ou les mêmes centres d'intérêt qu'un jeune de 12 ans qui arrive au lycée ou qu'un adolescent de 17 ans sur le point d'entrer dans l'âge adulte. A divers stades des présentes directives, nous avons adapté nos conseils ou nos recommandations afin de tenir compte de ces contextes différents. Bien que l'emploi de catégories vastes puisse utilement servir de guide, il ne faut jamais oublier qu'en fin de compte, tous les enfants sont différents. Les besoins spécifiques de chaque enfant doivent être pris en considération individuellement. De plus, de nombreux facteurs juridiques et culturels locaux sont susceptibles d'avoir une grande incidence sur la manière d'utiliser ou d'interpréter les présentes directives dans tel ou tel pays ou dans telle ou telle région.

Il existe désormais un important ensemble de règles de droit international et d'instruments internationaux qui étayent les mesures à prendre pour protéger les enfants tant en général que spécifiquement par rapport à Internet, et qui bien souvent rendent même ces interventions obligatoires. Ces lois et instruments constituent la base des présentes directives. Ils sont résumés de façon exhaustive dans la Déclaration de Rio de Janeiro et le Plan d'action pour prévenir et arrêter l'exploitation sexuelle des enfants et des adolescents, adopté lors du 3e Congrès mondial contre l'exploitation sexuelle des enfants et des adolescents, en novembre 2008.

«La protection des enfants sur Internet est un souci mondial qui appelle une réponse mondiale»

Avant-propos



Je suis ravi d'avoir l'occasion de vous présenter ces directives préliminaires, élaborées avec l'aide inestimable de nombreuses parties prenantes.

A une époque d'accès généralisé à Internet à haut débit, la protection de l'enfance en ligne est une question critique qui exige en urgence une réponse mondiale et coordonnée. S'il est vrai que des initiatives locales et même nationales ont assurément leur place, Internet ne connaît pas de frontières, de sorte que c'est la coopération internationale qui sera la clef de notre succès dans les batailles qui nous attendent.

Les enfants eux-mêmes, en utilisant leurs ordinateurs et leurs mobiles pour accéder à Internet, peuvent apporter une contribution énorme et nous aider à gagner la lutte contre le cybercrime et les cybermenaces. Je vous exprime personnellement ma reconnaissance pour votre soutien.

Hamadoun I. Touré

Secrétaire général de l'Union internationale des télécommunications (UIT)

Résumé analytique

La société de l'information dans laquelle les enfants et les adolescents grandissent actuellement offre un monde numérique disponible instantanément par un simple clic de souris. A un niveau inégalé, des services et des informations sont accessibles sur un ordinateur ou un dispositif mobile ayant accès à Internet. Les barrières associées au coût de ces dispositifs et à l'accès à Internet s'abaissent rapidement. Tous ces progrès techniques offrent aux enfants et aux adolescents des occasions inouïes d'explorer de nouvelles frontières et de faire des rencontres avec des personnes vivant très loin de chez eux. Les enfants et les adolescents sont réellement en train de devenir des citoyens numériques dans un monde en ligne qui ne connaît aucune frontière.

Le plus souvent, il s'agit là d'une expérience positive et formatrice, qui aide les jeunes générations à mieux comprendre ce qui différencie les peuples du monde aussi bien que ce qu'ils ont en commun. Mais les enfants et les adolescents doivent aussi être sensibilisés à certaines des facettes potentiellement négatives des progrès technologiques.

Parmi les activités préjudiciables peuvent figurer le harcèlement et les vexations, l'usurpation d'identité et l'abus en ligne (par exemple lorsque les enfants visualisent du contenu nocif et illégal, ou sont victimes de manipulation psychologique à des fins sexuelles, ou de la production, de la distribution et de la collecte de matériel constituant de la maltraitance à l'égard des enfants).

Toutes ces menaces pèsent sur le bien-être des enfants et des adolescents et représentent un défi qui doit être relevé par toutes les parties prenantes, y compris les enfants eux-mêmes.

Alors que tous les fournisseurs de services en ligne doivent faire tout ce qu'ils peuvent sur le plan technique pour rendre Internet aussi sûr que possible pour les enfants et les adolescents, la première et la meilleure forme de défense pour VOUS protéger consiste à vous sensibiliser à ce qui peut arriver en ligne et à vous faire comprendre qu'il y a toujours une solution à un problème rencontré sur Internet. C'est pourquoi il est de la plus haute importance de responsabiliser les enfants et les adolescents par le biais de mesures éducatives et de sensibilisation.


ABCDEFGHIJKLM
2345678901234567
OVELOVELOVELOVE
1 2 3

Les présentes directives ont été préparées dans le contexte de l'initiative pour la Protection de l'enfance en ligne (COP)[1] en vue de jeter les bases d'un cybermonde sûr et sans danger non seulement pour les enfants d'aujourd'hui, mais aussi pour les générations futures. Elles sont destinées à servir de prototype pouvant être adapté et utilisé en cohérence avec les lois et coutumes nationales ou locales. De plus, il convient de voir que ces directives abordent des questions qui sont susceptibles d'affecter tous les enfants et les adolescents de moins de 18 ans, mais que chaque tranche d'âge a des besoins différents. En fait, chaque enfant est unique, et mérite une considération individuelle.

Les présentes directives mondiales destinées aux enfants et aux adolescents ont été élaborées par l'UIT et une équipe d'auteurs issus d'éminentes institutions actives dans le secteur des TIC, par exemple *Save the Children*, Interpol et Telefónica, CHIS et INSAFE.

La Convention des Nations Unies sur les droits de l'enfant[2] et spécifiquement les résultats du SMSI ont reconnu les besoins des enfants et des adolescents et la nécessité de les protéger dans le cyberespace. L'engagement de Tunis a reconnu «le rôle des TIC dans la protection et le développement des enfants» ainsi que la nécessité de renforcer l'action pour «protéger les enfants contre tout abus et assurer la défense de leurs droits dans le contexte des TIC».

En publiant les présentes directives, l'initiative COP demande à toutes les parties prenantes, y compris les enfants et les adolescents, de promouvoir l'adoption de politiques et de stratégies qui protègent les enfants dans le cyberespace et assurent un accès plus sûr à toutes les opportunités et ressources extraordinaires qui sont disponibles en ligne.

Espérons que cela aboutira non seulement à édifier une société de l'information plus inclusive, mais que cela permettra aussi aux pays de satisfaire à leurs obligations en matière de protection et de réalisation des droits des enfants tels qu'énoncés dans la Convention des Nations Unies sur les droits de l'enfant, adoptée par la résolution 44/25 du 20 novembre 1989 de l'Assemblée générale des Nations Unies, et dans le document de résultat du SMSI.

[1] www.itu.int/cop
[2] www.unicef.org/crc/


e
WWW

1. Arrière-plan

La Convention des Nations Unies sur les droits de l'enfant, approuvée par les Nations Unies en 1989, est le plus important outil juridique pour défendre et promouvoir les droits des enfants et des adolescents. Elle met l'accent sur les besoins réels, non seulement en termes de vulnérabilité et de mesures de protection, mais aussi s'agissant de la promotion et de l'appréciation des aptitudes de chaque enfant et de chaque adolescent.

Le Sommet mondial sur la société de l'information (SMSI) qui s'est tenu en deux temps, à Genève du 10 au 12 décembre 2003 et à Tunis du 16 au 18 novembre 2005, s'est conclu par l'approbation de résultats qui prennent un audacieux engagement «à édifier une société de l'information à dimension humaine, inclusive et privilégiant le développement», où chacun puisse créer des informations et des connaissances, y accéder, les utiliser et les partager.

Au SMSI, l'UIT a été chargée par les dirigeants de la communauté internationale de s'occuper de la Grande Orientation C5: «améliorer la confiance et la sécurité dans l'utilisation des TIC». Les résultats du SMSI ont également spécifiquement reconnu les besoins des enfants et des adolescents et la nécessité de les protéger dans le cyberespace. L'Engagement de Tunis a reconnu «le rôle des TIC dans la protection et le développement des enfants» ainsi que la nécessité de renforcer l'action pour «protéger les enfants contre tout abus et assurer la défense de leurs droits dans le contexte des TIC».

Par ailleurs, la communauté mondiale des enfants et des adolescents a déclaré ce qui suit dans le document de résultat du 3e Congrès mondial contre l'exploitation sexuelle des enfants et des adolescents[3], tenu au Brésil en 2008: «Nous demandons des règles de cybersécurité plus fortes et qui soient bien propagées tant sur les sites web qu'à l'intérieur des communautés. A cette fin, nous réclamons l'élaboration accrue de manuels pour les enfants, les enseignants, les parents et les familles, abordant les menaces d'Internet tout en fournissant des informations supplémentaires sur l'exploitation sexuelle des enfants».

Les technologies en ligne offrent de nombreuses possibilités de communiquer, d'apprendre de nouvelles compétences, d'exercer sa créativité et de contribuer à instaurer une société meilleure pour tous, mais souvent, elles créent également de nouveaux risques, par exemple en exposant les enfants et les adolescents à des dangers potentiels tels que le contenu illégal, les virus, le harcèlement (par exemple dans les chat rooms), l'utilisation frauduleuse de données personnelles ou la manipulation psychologique (*grooming*) à des fins sexuelles.

Il n'existe pas de panacée pour protéger les enfants en ligne. Il s'agit là d'un problème mondial qui exige une réponse mondiale émanant de tous les segments de la société, y compris les enfants et les adolescents eux-mêmes.

3 www.ecpat.net/WorldCongressIII/PDF/Outcome/WCIII_Outcome_Document_Final.pdf

Etude de cas: la voix des enfants et des adolescents

Le 3e Congrès mondial contre l'exploitation sexuelle des enfants et des adolescents s'est tenu à Rio de Janeiro, Brésil, du 25 au 28 novembre 2008. Il a rassemblé 3 500 participants y compris 300 adolescents, dont 150 venant de pays étrangers.

Il s'est conclu par un document de résultat appelé «Déclaration de Rio de Janeiro pour prévenir et arrêter l'exploitation sexuelle des enfants et des adolescents», qui contient la «Déclaration des adolescents pour mettre fin à l'exploitation sexuelle». Voici quelques-uns des principaux messages que les enfants et les adolescents adressent au monde:

Nous, les enfants du monde, remercions le Gouvernement du Brésil et les autres gouvernements et institutions responsables, de nous avoir donné, à nous, les enfants, présent et avenir du monde, une voix à ce 3e Congrès mondial.

...

7. Nous lançons un appel pour que les gouvernements agissent afin d'adopter des lois et des politiques qui apportent des bienfaits aux enfants et en assurent la protection et le bien-être, tant au plan local qu'au plan international. Cependant, il ne suffit pas de permettre aux gouvernements de faire des promesses creuses pour juguler ces attaques contre les enfants. Par conséquent, nous, les enfants, demandons que des comités d'action soient créés pour auditer les plans d'action dans chaque pays.

8. Nous lançons également un appel pour l'adoption d'une Journée internationale où les enfants dirigent les efforts lors des campagnes de sensibilisation, de rassemblements et de défilés. Afin d'élargir encore la portée de cette journée, nous demandons que soit organisé un concours international d'expression artistique, écrite et orale qui culminera ce jour-là.

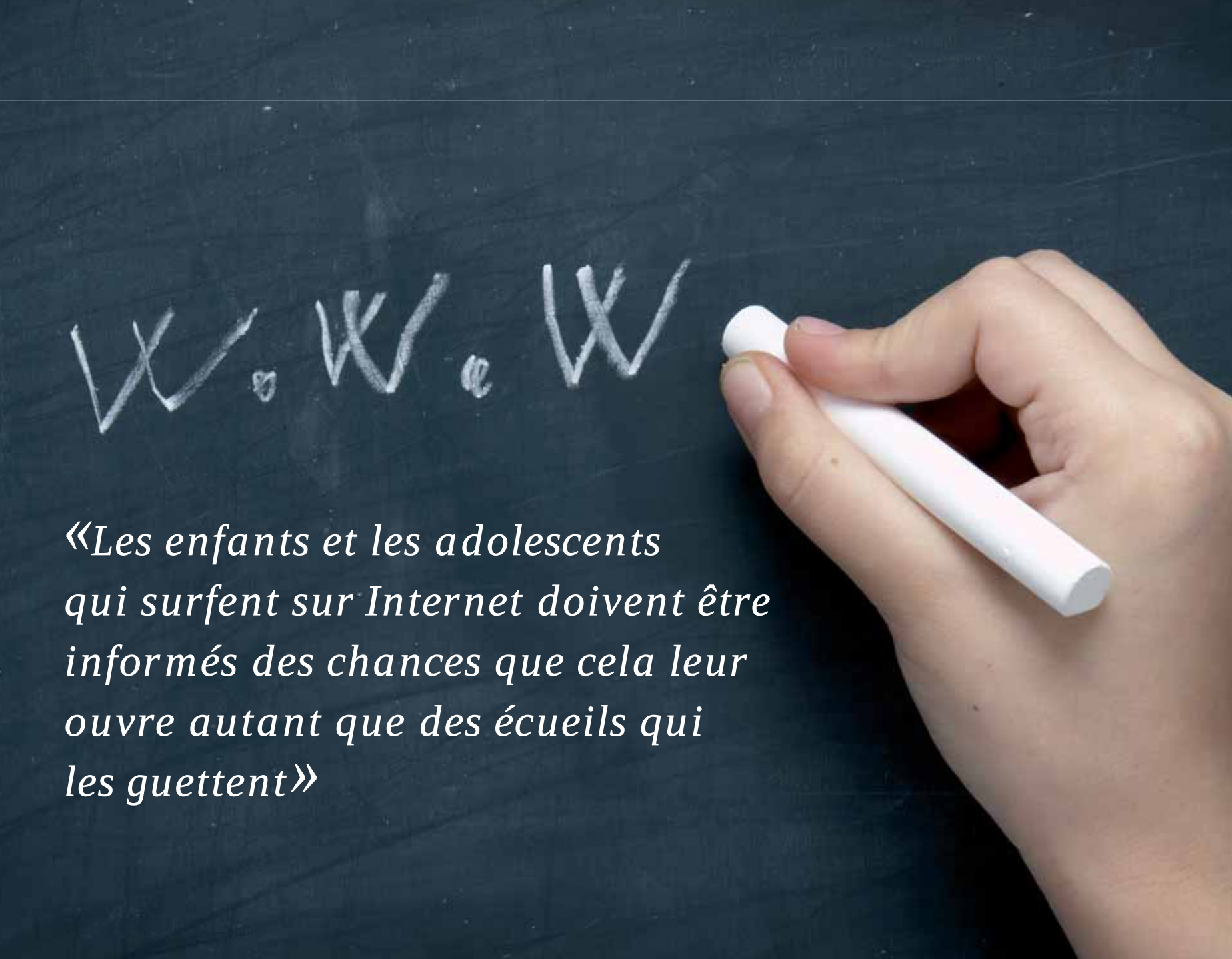
9. Nous portons désormais notre attention sur les médias, en particulier l'Internet, qui pose une des plus grandes menaces à des millions d'enfants dans le monde entier.

10. Nous, les enfants, devons faire connaître notre situation critique pour que les gouvernements poursuivent une législation stricte et punitive en matière d'Internet, en particulier s'agissant de la pornographie infantile, qui n'est qu'une une autre forme d'abus.

11. De même, nous demandons des règles de cybersécurité fortes qui soient bien propagées tant sur les sites web qu'à l'intérieur des communautés. A cette fin, nous lançons un appel pour l'élaboration accrue de manuels pour les enfants, les enseignants, les parents et les familles et qui abordent les menaces d'Internet tout en fournissant des informations supplémentaires sur l'exploitation sexuelle des enfants.

12. Par ailleurs, nous donnons mandat aux médias pour rassembler des documents, rapports, dossiers, CD, vidéos et autres matériels pour améliorer les connaissances sur cette question. Nous, les enfants du monde, nous engageons avec véhémence et passion à poursuivre ces politiques et à demander à nos gouvernements d'agir si nous ne constatons pas que des démarches positives sont prises afin de mettre fin à ce phénomène qui continue à tourmenter le monde aujourd'hui.

La «Déclaration pour mettre fin à l'exploitation sexuelle» figure à l'adresse:
www.iiicongressomundial.net/congresso/arquivos/Rio%20Declaration%20and%20Call%20for%20Action%20-%20FINAL%20Version.pdf



«Les enfants et les adolescents qui surfent sur Internet doivent être informés des chances que cela leur ouvre autant que des écueils qui les guettent»

2. Les enfants et les adolescents en ligne

Les technologies de l'information et de la communication (TIC) sont en train de changer la manière dont les enfants interagissent avec leurs pairs, dont ils accèdent à l'information, dont ils expriment leurs avis, dont ils affichent et partagent du contenu créatif. Les enfants et les adolescents apprécient tout particulièrement la nature éminemment interactive de bon nombre de services liés à la Toile. En général, ils considèrent Internet avec un sentiment de sécurité, comme quelque chose qu'ils apprécient, qui les intéresse, qui les amuse, qui les détend, qui leur est utile et qu'ils jugent amical[4].

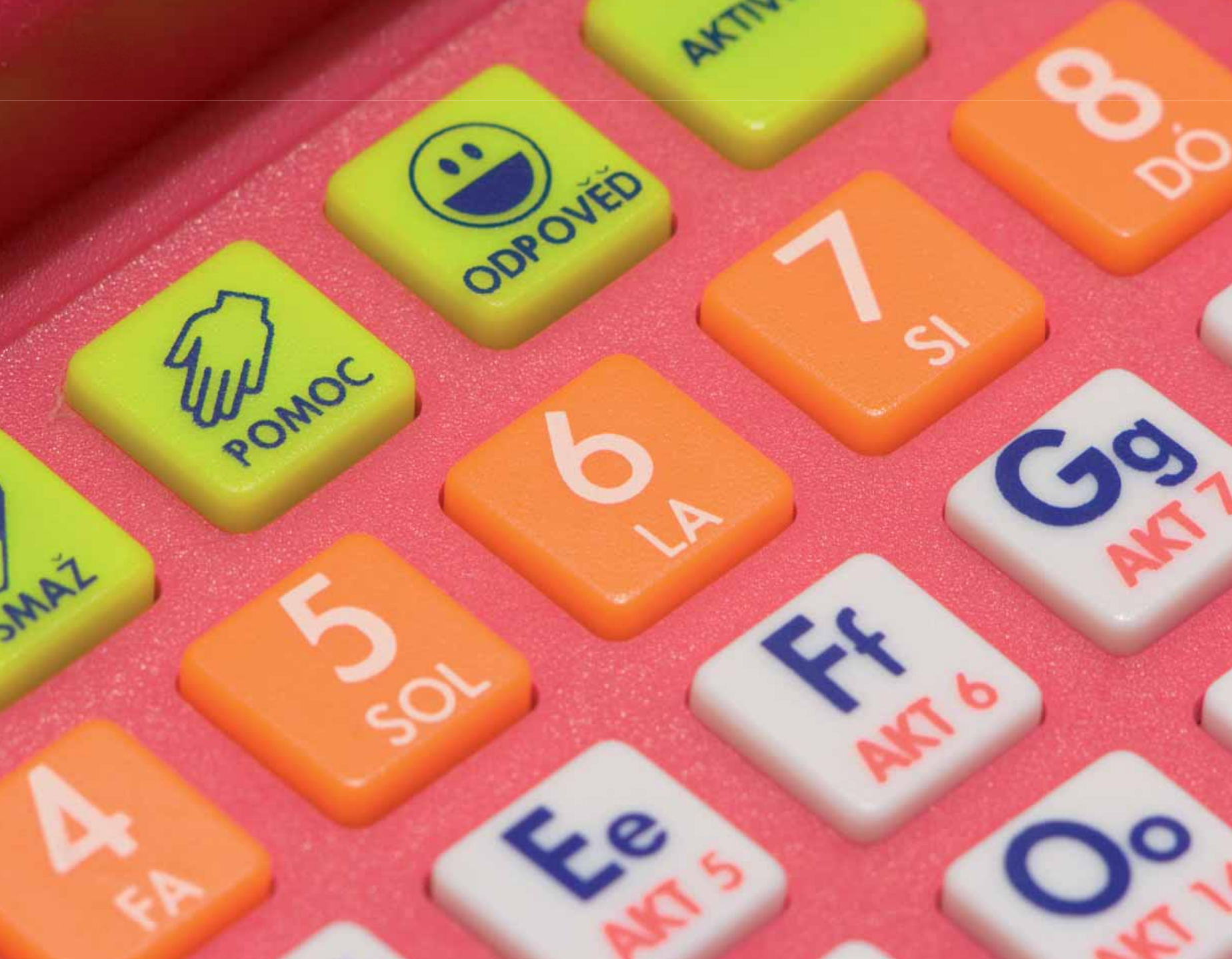
Accès

Une étude danoise[5] a constaté que «au fur et à mesure que les enfants grandissent, leur utilisation d'Internet s'accroît. Dix-neuf pour cent des enfants entre 9 et 10 ans ayant répondu utilisent Internet chaque jour. Par comparaison, 80% des 14 à 16 ans utilisent Internet quotidiennement». Une tendance similaire est observée à Singapour[6], où 56% des enfants de 5 à 14 ans disent surfer sur Internet tous les jours. L'activité préférée sur Internet semble être la recherche d'informations liées aux passe-temps et aux intérêts personnels, la participation à des jeux ainsi que les recherches destinées aux devoirs à l'école.

[4] www.childresearch

[5] www.saferinternet.org/ww/en/pub/insafe/news/articles/0409/digital_life.htm

[6] www.itu.int/ITU-D/ict/material/Youth_2008.pdf (page 62).


POMOC
ODPOVĚĎ
SMAŽ
4
FA
5
SOL
6
LA
7
SI
8
Gg
Ff
AKT 6
Fe
AKT 5
Oo

L'accès fixe à haut débit, largement disponible, reste encore la manière préférée d'aller sur Internet dans les pays développés, par comparaison avec les pays en développement, où ce genre d'infrastructures est moins développé et où l'accès mobile à Internet est déjà le mode d'accès usuel et gagnera encore en importance. Dans de nombreux pays, les cybercafés et les autres ressources communales constituent également d'importantes sources d'accès pour les enfants et les adolescents et le resteront sans doute encore quelque temps. Dans l'Union européenne, 50% des enfants de 10 ans, 87% des jeunes de 13 ans et 95% des adolescents de 16 ans ont un téléphone portable[7]. Dans la région Asie-Pacifique, qui connaît la croissance la plus rapide en matière d'abonnements mobiles, la Chine et l'Inde sont devenus les leaders de cette technologie avec un taux de croissance de six millions de mobiles par mois rien qu'en Inde[8]. Les connexions mobiles se chiffrent désormais à quatre milliards dans le monde, dont près de 100 millions incluent le haut débit mobile[9]. Il est clair que l'aptitude à accéder à des services en ligne va de plus en plus passer par des dispositifs portables.

Les avantages sont évidents: toute une gamme de services éducatifs pourrait être dispensée aux enfants des villages et des communautés reculés par le biais de mobiles. Les téléphones portables pourraient jouer un rôle essentiel pour connecter les enfants les uns aux autres à des fins éducatives et d'apprentissage avec leurs pairs. Ils sont particulièrement importants pour les communautés nomades ou déplacées par suite de catastrophes naturelles, de guerres civiles ou d'autres perturbations majeures.

Dispositifs numériques

Une récente étude réalisée dans les foyers latino-américains a montré que la génération la plus jeune est très bien équipée[10].

Outre les ordinateurs et les téléphones cellulaires, de nombreux autres dispositifs électroniques permettent d'accéder à Internet ou vont bientôt le permettre. Voici une sélection des dispositifs que les participants à l'enquête possèdent chez eux:

Equipement à domicile	Tranche de 6 à 9 ans	Tranche de 10 à 18 ans
Un ordinateur chez soi	61%	65%
Connexion à Internet	40%	46%
Téléphone cellulaire personnel	42%	83%

7 europa.eu/rapid/pressReleasesAction.do?reference=IP/09/596

8 www.tigweb.org/express/panorama/article.html?ContentID=11441

9 gsmworld.com/newsroom/press-releases/2009/2521.htm#nav-6

10 www.generacionesinteractivas.org/?page_id=660

Information

L'accès à l'information est crucial pour les enfants et les adolescents qui doivent faire leurs devoirs. Une étude sur l'utilisation d'Internet par les enfants japonais[11] indique que 70% d'entre eux y ont recours pour faire leurs devoirs. Les bibliothèques sont devenues virtuelles et la capacité à y trouver des informations pertinentes et fiables dans n'importe quelle langue est un grand avantage qui a été embrassé par les jeunes du monde entier. Une des ressources en ligne les plus utilisées est Wikipedia[12]. Wikipedia est un projet d'encyclopédie multilingue sur le web, à contenu libre, où il est possible de lire, de modifier et de rédiger des articles sur n'importe quel sujet ou question jugée pertinente. La recherche d'informations peut aisément faire passer sans arrêt d'une page à une autre. La quête d'informations nouvelles n'est jamais ennuyeuse et les barrières linguistiques disparaissent peu à peu grâce à la localisation croissante du contenu.

Réseaux sociaux

La naissance des réseaux sociaux en ligne a été un remarquable succès. La diversité des réseaux sociaux couvre tous les âges, toutes les cultures et toutes les langues. Le fait d'avoir un profil sur un réseau social est devenu une facette importante de la vie en ligne de nombreux enfants et adolescents. De retour de l'école, ils peuvent ainsi continuer à discuter avec leurs amis en ligne tout en faisant leurs devoirs, envoyer des SMS et écouter de la musique (souvent en même temps!).

Les réseaux sociaux peuvent souvent représenter une passerelle unique menant à des jeux, des amis, des actualités, de la musique et des manières d'exprimer sa créativité. En d'autres termes, on peut se montrer créatif, s'amuser, réfléchir et se divertir en utilisant les TIC.

On pourrait prendre l'exemple d'un jeune groupe de musiciens qui crée une nouvelle chanson, la met en ligne sur MySpace[13] et en informe ses amis et ses fans. Ces derniers peuvent alors écouter la chanson diffusée en ligne en continu, ou la télécharger sur leur lecteur mp3 ou leur téléphone portable pour l'écouter en chemin. Si la chanson leur plaît, ils en parleront autour d'eux à leurs amis, qui le diront à leur tour à leurs amis, et ainsi de suite. Avec des techniques simples et un investissement financier limité, ce groupe peut dès lors élargir sa base de fans et être potentiellement écouté par une société de disques susceptible de les recruter. On ne compte désormais plus les cas de groupes qui ont assuré la promotion de leurs chansons par le biais de services tels que MySpace et ont fini par signer un contrat pour enregistrer un disque.

Cela n'est pas si différent du monde réel, mais l'un des grands avantages des TIC est qu'elles permettent d'atteindre un public plus large en moins de temps. Essentiellement, un service peut décoller lentement mais atteindre une masse critique mondiale en très peu de temps grâce à la capacité des enfants et des adolescents à partager instantanément leurs expériences avec leurs amis.

Mondes virtuels pour les enfants et les adolescents

Dans ces mondes, les enfants peuvent souvent créer un avatar et, grâce à lui, explorer un univers imaginaire. Ils peuvent jouer à

11 www.childresearch.net/RESOURCE/RESEARCH/2008/KANOH2_1.HTM

12 en.wikipedia.org/wiki/Main_Page

13 www.myspace.com/

des jeux, bavarder et décorer des chambres virtuelles ou d'autres espaces. Selon la société de consultance *K Zero*, il existera, à la fin de 2009, 70 millions de comptes uniques, deux fois plus que l'an dernier, dans des mondes virtuels qui s'adressent aux enfants de moins de 16 ans. *Virtual Worlds Management*, une société de médias et d'événementiel commercial, estime qu'il existe désormais plus de 200 mondes virtuels axés sur les jeunes «en activité, prévus ou en cours de développement actif»[14].

Les mondes virtuels, tels que *Habbo Hotel* [15], qui cible les adolescents, permettent aux utilisateurs de créer un profil et d'être représentés dans le cybermonde par un avatar[16]. Tous les utilisateurs sont appelés à créer leur propre avatar à l'aide d'outils faciles à utiliser. La capacité de se présenter en tant qu'avatar permet à chacun, quelle que soit son apparence physique dans le monde réel, d'entrer dans une communauté où tous sont égaux et où les préjugés n'existent pas.

Grâce à cette nouvelle identité, l'utilisateur peut s'exprimer différemment, tester un nouveau profil ou une nouvelle attitude, faire preuve d'audace et de franchise sur des questions qui lui tiennent à cœur, ou simplement vivre «la vie de quelqu'un d'autre» pendant quelque temps.

Inutile de dire qu'il existe des règles à observer, mais la possibilité de tester une personnalité différente peut s'avérer une expérience amusante.

Quel est ton profil en ligne?

Une étude intéressante[17] réalisée avec les utilisateurs de *Habbo Hotel* révèle le profil numérique des adolescents en ligne:

Entrepreneurs	Ambitieux, décidés et matérialistes. Ils accordent de la valeur au succès matériel et bien qu'ayant de nombreux amis, n'accordent pas aux sentiments des autres autant de considération que d'autres segments.
Rebelles	Accordent de la valeur à l'accumulation d'un grand nombre d'expériences dans la vie et au fait de mener un style de vie au rythme soutenu. Comme les entrepreneurs, ils veulent devenir «riches et célèbres», mais ne sont pas disposés à renoncer au plaisir pour atteindre cet objectif.
Traditionnels	Accordent de la valeur à une vie ordinaire et se voient comme honnêtes, polis et obéissants. Ils sont désireux d'aider les autres mais sont moins ambitieux et recherchent moins le plaisir que d'autres segments.
Créatifs	Partagent bon nombre des mêmes traits positifs que les traditionnels, mais en mettant l'accent sur la créativité. Ils accordent de la valeur à la qualité de l'éducation reçue et à l'influence qu'ils peuvent exercer dans la vie, mais sont également actifs, sociaux et manifestent de l'intérêt pour les voyages.
Solitaires	Plus introvertis et moins susceptibles que les autres segments de s'identifier à des traits de personnalité particuliers. Ils se voient rarement comme actifs ou assurés, mais sont plus ouverts d'esprit dans leurs attitudes que les traditionnels ou les entrepreneurs.

[14] www.nytimes.com/2009/04/19/business/19proto.html?_r=1&emc=eta1

[15] www.habbo.com/

[16] Dans les jeux vidéo, les avatars sont essentiellement la représentation physique du joueur dans le monde du jeu. http://en.wikipedia.org/wiki/Avatar_(computing)

[17] www.sulake.com/press/releases/2008-04-03-Global_Habbo_Youth_Survey.html

Les enfants et les adolescents ont des profils en ligne et communiquent entre eux en postant des commentaires ou des salutations sur les pages de profils de leurs amis. Il semble bien que le fait d'avoir de nombreux amis reliés à son profil donne un statut plus élevé parmi les pairs, même si l'on peut se demander si le nombre important d'amis en ligne constitue en soi un objectif à rechercher. Il n'en reste pas moins que 74% des jeunes Danois de 14 à 16 ans ont déclaré qu'ils commentaient les profils des autres en ligne[18], et une tendance similaire s'observe dans des sites de réseaux sociaux mondiaux tels que *Facebook* [19], *Hi5* [20] ou *Bebo* [21], où une grande part de l'interaction sur ces sites consiste à poster des commentaires sur les profils des autres.

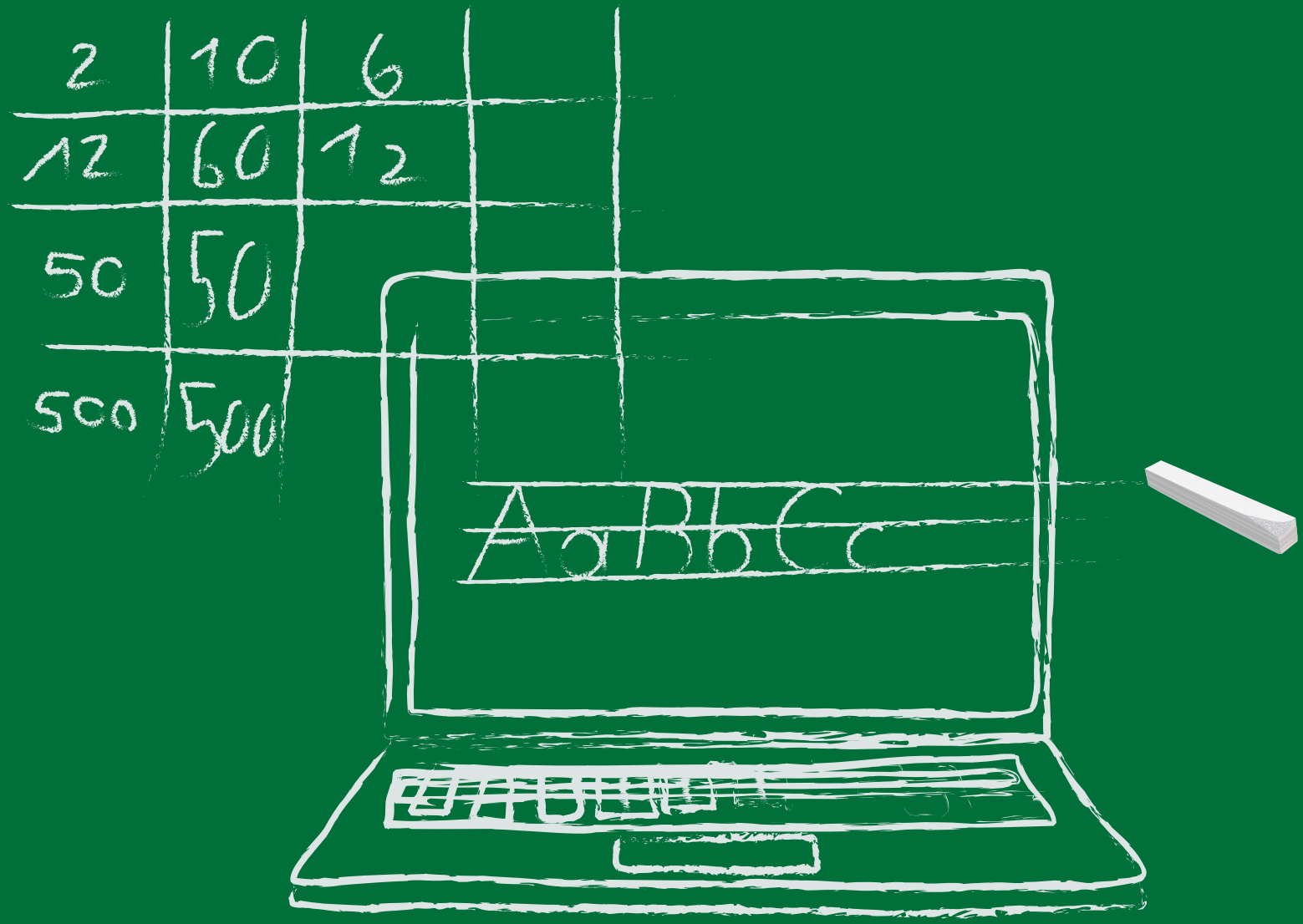
De nombreux réseaux sociaux facilitent la création de sous-groupes axés sur des thèmes tels que la démocratie, les animaux domestiques, les jeux, le travail à l'école, la musique et ainsi de suite. Il est possible que ces communautés ne soient pas disponibles dans toutes les villes, les régions ou les pays, mais, une fois encore, les TIC condensent le monde pour l'apporter sur votre écran et vous offrent la possibilité d'expérimenter des formes de participation et de liberté d'expression qui sont rarement garanties au quotidien dans la vie réelle du monde adulte. La culture positive qui règne dans les communautés en ligne aide tout le monde à faire des expériences agréables et incite davantage au dialogue en ligne et à l'apprentissage de choses nouvelles.

[18] www.saferinternet.org/ww/en/pub/insafe/news/articles/0409/digital_life.htm

[19] www.facebook.com/

[20] hi5networks.com/

[21] www.bebo.com/


2 10 6
12 60 12
50 50
500 500
AaBbCc

Etude de cas: le bon côté des réseaux sociaux pour les enfants présentant des difficultés d'apprentissage

Les avantages concrets des réseaux sociaux pour les enfants présentant des difficultés d'apprentissage peuvent être résumés de la façon suivante:[22]

Pratique de compétences sociales: l'enfant a l'occasion de rencontrer toutes sortes de gens en ligne. Du fait que la socialisation par le biais de la technologie n'est pas aussi immédiate que les interactions personnelles ou les conversations téléphoniques, il a un peu plus de temps pour réfléchir à une situation avant d'y réagir. Cela lui donne l'occasion d'expérimenter avec les salutations, les réponses, etc.

Interaction sociale définie / guidée: alors que les technologies de la communication en ligne permettent de plus en plus une interaction dépourvue de formes, l'interaction sociale peut être restreinte (sur les plans du périmètre d'application et de la sécurité). Parmi les exemples d'interaction focalisée en ligne, citons les listes de copains / amis, les chat rooms thématiques avec présence d'un animateur ou les forums de discussion et, pour les plus jeunes, l'occasion donnée aux parents d'aider l'enfant en tapant au clavier ou en lui lisant les textes à l'écran pendant un certain temps. Cela peut aider l'enfant à stabiliser ses compétences et sa confiance, ce qui accroîtra son degré d'indépendance au fur et à mesure de sa maturation.

Expérimentation d'identité: l'enfant peut se créer une identité en ligne différente de son identité normale. Ainsi, un enfant qui adore les bandes dessinées peut être sur Internet «le roi de la connaissance des super-héros» sans s'exposer aux taquineries de ses camarades de classe. Cet enfant peut aussi trouver un groupe d'enfants du même âge qui apprécie cet aspect de sa personnalité.

Utilisation fréquente de technologies existantes et émergentes / en mutation. La technologie évolue plus vite que jamais. En apprenant à s'adapter à de nouvelles technologies (ou à des applications nouvelles de technologies existantes), l'enfant sera mieux équipé pour s'adapter aux technologies futures. Cela l'aidera à apprécier rapidement les risques de communiquer par le biais de ces nouvelles méthodes et à adapter son comportement afin de conserver le contrôle sur sa propre sécurité.

[22] www.greatschools.net / cgi-bin / showarticle / 3120

Jeux

Les jeux de société classiques se sont également implantés sur le net, et sont désormais pratiqués parallèlement à ce que l'on appelle les «jeux de rôles multi-joueurs massivement en ligne» (MMORPG). Comme pour les réseaux sociaux, les jeux en ligne peuvent connecter à d'autres joueurs venant du monde entier. Ils constituent en fait une activité sociale qui captive la jeunesse universelle. Le terme de «joueur en ligne» peut évoquer l'image d'un adolescent solitaire jouant à «Ever-Quest» dans le sous-sol de la maison familiale, mais ce n'est pas ainsi que cela se passe en Corée du Sud. Dans ce pays, l'interaction de groupe est une tradition culturelle aussi forte que les études ou le shopping. Les jeunes vont dans les cybercafés pour décompresser et passer du temps ensemble. «La communauté au sein des jeux est réellement populaire, tout comme l'aptitude à former des groupes ou des guildes», déclare Luong. «Ces aspects sociaux sont une importante raison pour laquelle les gens jouent à des jeux [en Corée du Sud].»[23]

Citoyenneté numérique

L'introduction de nouvelles technologies implique toujours la nécessité de savoir les utiliser à bon escient. Nous tous, y compris les enfants et les adolescents, pouvons exiger que les producteurs et les fournisseurs incorporent autant de caractéristiques de sécurité que possible, afin de nous permettre de faire des choix éclairés sur des questions telles que, par exemple, la révélation d'informations privées. Mais il incombe aux enfants et aux adolescents d'assumer l'essentiel de la responsabilité d'un comportement convenable et respectueux en ligne. On emploie de plus en plus à cet effet le terme de citoyenneté numérique. La citoyenneté numérique ne consiste pas simplement à reconnaître et à traiter les risques en ligne. Elle vise à créer des espaces et des communautés sûrs, à comprendre comment gérer l'information personnelle et être rompu à l'Internet – en utilisant sa présence en ligne pour se développer et façonner son propre monde en toute sécurité, de façon créative, et en stimulant les autres à faire de même[24].

Internet sans crainte

Chaque année, le monde célèbre l'utilisation positive et plus sûre d'Internet. De telles manifestations peuvent impliquer les enfants, les écoles locales, l'industrie et les acteurs pertinents qui, tous, contribuent à sensibiliser aux bienfaits des expériences en ligne. Pour des informations à jour sur ces manifestations, il est suggéré de faire une recherche en ligne avec les termes «*Internet safety celebration*» + «nom du pays».

[23] www.msnbc.msn.com/id/17175353/

[24] www.digizen.org/

«Etre futé, responsable et en sécurité sur Internet – tout comme dans le monde réel»

Voici une liste de questions à aborder pour discuter de la «citoyenneté numérique»

Etiquette numérique: normes électroniques de conduite ou de procédure.

- Il ne suffit pas d'établir des règles et des politiques, nous devons apprendre à devenir responsables au sein de cette nouvelle société.

Communication numérique: échange électronique d'informations.

- Tout le monde doit avoir l'occasion d'accéder à l'information, où qu'elle soit et à tout moment.

Culture numérique: processus consistant à enseigner et à apprendre la technologie et la manière de l'utiliser.

- Au fur et à mesure de l'apparition de nouvelles technologies, nous devons apprendre à les utiliser rapidement et convenablement. Nous devons acquérir une bonne culture numérique.

Accès numérique: pleine participation électronique à la société.

- Toute forme d'exclusion numérique entrave le développement des êtres humains dans une société électronique. Il ne faut pas qu'un des deux sexes bénéficie d'un traitement préférentiel par rapport à l'autre. L'accès électronique ne doit pas être déterminé par la race, le handicap physique ou mental. La question des personnes vivant dans des villes ayant une connectivité limitée doit être également réglée. Pour devenir des citoyens productifs, nous devons être attachés à l'égalité devant l'accès au numérique.

Commerce numérique: achat et vente de marchandises par voie électronique.

- Les enfants et les adolescents doivent apprendre à être des consommateurs efficaces dans une économie numérique sûre.

Droit numérique: responsabilités électroniques des actes.

- Le droit numérique traite de l'éthique de la technologie. Il existe certaines règles de la société qui répriment des actes délictuels. Ces lois s'appliquent à tout le monde qui travaille ou joue en ligne.

Droits et responsabilités numériques: achat et vente de marchandises par voie électronique.

- Les droits numériques fondamentaux doivent être étudiés, discutés et compris dans le monde numérique. Ces droits sont également assortis de responsabilités. Les utilisateurs, y compris les enfants et les adolescents, doivent contribuer à définir la bonne manière d'utiliser la technologie. Dans une société numérique, ces deux domaines doivent aller de pair pour que tout le monde puisse être productif.

Sécurité numérique (auto-protection): précautions électroniques pour garantir la sécurité.

- Dans toute société, il existe des individus qui commettent des vols ou des dégradations ou qui perturbent la vie d'autrui. La communauté numérique ne fait pas exception. Il ne suffit pas de faire confiance à ses pairs au sein de la communauté pour être en sécurité. A la maison, nous mettons des verrous aux portes et nous installons des alarmes incendie afin d'assurer un certain degré de protection. Il doit en être de même dans le monde numérique afin d'assurer la protection et la sécurité numérique. Nous devons avoir des protections contre les virus, des sauvegardes de données et le contrôle de crête de notre équipement. En tant que citoyens responsables, nous devons protéger notre information contre des forces extérieures susceptibles de provoquer des perturbations ou des dégâts.

Source: www.digitalcitizenship.net / Nine_Elements.html

«Tous les enfants et les adolescents du monde ont le droit de surfer en toute sécurité»

3. Ce qu'il faut savoir pour rester en sécurité en ligne

DIRECTIVES SUR LA SÉCURITÉ SUR INTERNET

Les messages de sécurité sur Internet doivent arriver à temps, être adaptés à l'âge, respecter les sensibilités culturelles et correspondre aux valeurs et aux lois de la société où vit l'enfant ou l'adolescent.

L'initiative COP a identifié trois principales tranches d'âge pour les jeunes internautes. Ces groupes correspondent *grosso modo* aux stades principaux du développement d'un enfant sur la voie menant à l'âge adulte. De ce fait, les directives peuvent être vues comme une échelle qui fait traverser à l'enfant des phases progressives. On ne saurait cependant trop insister sur le fait que chaque enfant est différent et exige et mérite une attention individuelle. Il n'y a pas de taille unique convenant à tout le monde. Rien ne doit jamais être supposé *a priori* ni considéré comme acquis

Première tranche d'âge, de 5 à 7 ans

Ce groupe fait l'expérience de ses premiers contacts avec la technologie. Son usage doit être étroitement surveillé à tout moment par un parent ou un adulte. Les logiciels de filtrage ou les autres mesures techniques peuvent également jouer un rôle utile pour accompagner l'utilisation d'Internet

par un enfant de cet âge. Il serait sage d'envisager de limiter l'accès potentiel d'un enfant aussi jeune, par exemple en dressant la liste des sites web sûrs et adaptés à son âge, comme un mur entourant un jardin. Le but est de fournir aux enfants de cet âge les règles de base de la sécurité sur Internet, de l'étiquette et de la compréhension. Cette tranche d'âge ne sera sans doute pas en mesure de décoder des messages plus sophistiqués. Les parents ou les adultes responsables d'enfants devraient consulter les directives COP destinées aux parents, aux tuteurs et aux éducateurs, afin de voir comment aider au mieux les plus jeunes à surfer en toute sécurité.

Deuxième tranche d'âge: de 8 à 12 ans

Cette période constitue une transition stimulante pour l'enfant. En règle générale, l'enfant est en train de devenir une jeune personne, présentant une plus grande capacité à formuler des questions. Sa curiosité l'incite à chercher et à remettre en cause les limites, en essayant de trouver ses propres réponses. C'est une tranche d'âge désormais sensibilisée à ce qui est disponible en ligne, et qui ressent une formidable impulsion à découvrir ce qui existe. Tout au long de son développement, l'enfant est censé tester les barrières et évoluer grâce à ce type d'apprentissage. Les logiciels de filtrage ou autres mesures techniques peuvent avoir un rôle particulièrement utile à jouer pour soutenir l'utilisation d'Internet par un jeune de cet âge. Une caractéristique importante des enfants de cette tranche d'âge est leur approche parfois peu critique du contenu et des contacts, ce qui peut les mettre dans une position particulièrement vulnérable face aux prédateurs et aux entités commerciales désireuses de les séduire.

Dernière tranche d'âge: 13 ans et plus

Ce groupe, qui couvre le plus grand nombre d'années, est composé de jeunes, et notamment d'adolescents. En rapide croissance, les jeunes de ce groupe sont en train de se transformer en adultes. Ils se développent tout en explorant leur propre identité, leurs propres goûts. Très souvent, ils sont capables d'utiliser la technologie avec un degré de compétence élevé, sans aucune surveillance ni interaction de la part d'adultes. Les logiciels de filtrage commencent à devenir moins utiles et moins pertinents, mais peuvent certainement continuer à jouer un rôle de soutien important, en particulier pour certains jeunes susceptibles de présenter des vulnérabilités temporaires ou prolongées.

En liaison avec leur propre développement hormonal et le sentiment croissant de leur maturité physique, les adolescents peuvent traverser des phases où ils ressentent un très fort besoin de trouver leur propre voie, d'échapper à la surveillance étroite des parents ou des adultes et de rechercher la compagnie de camarades du même âge. Une curiosité naturelle sur les questions liées à la sexualité peut inciter certains adolescents de cette tranche d'âge à se mettre dans des situations potentiellement inquiétantes. Il est donc d'autant plus important qu'ils comprennent comment rester en sécurité sur Internet.

Les directives COP reconnaissent la difficulté de créer des messages qui couvrent les besoins de tous les âges au sein des groupes définis. Les lois et coutumes locales sont également d'une grande importance dans ce genre de questions.

Il n'existe pas de taille unique qui puisse convenir à tous.

L'initiative pour la Protection de l'enfance en ligne serait très heureuse de pouvoir contribuer à adapter et à localiser le contenu des présentes directives ainsi que de toute autre directive COP. Si vous souhaitez donner suite à cette idée, n'hésitez pas à contacter cop@itu.int


SMART

“Règles SMART”

C’est très amusant de surfer sur Internet. Profitez-en tout en restant en sécurité.

1. On peut faire beaucoup de choses super sur Internet. On peut jouer, discuter avec des copains, se faire de nouveaux amis et trouver beaucoup d’informations utiles. Vous avez le droit de profiter de tout ce qu’Internet a à offrir et d’explorer tout cet univers.

2. Mais vous devez aussi savoir que l’on peut trouver des choses déplaisantes sur Internet, par exemple des images et des textes susceptibles de vous désorienter ou même de vous effrayer. Vos amis et les adultes en qui vous avez confiance ne sont pas les seules personnes qui sont présentes dans ce monde numérique. Malheureusement, Internet est aussi utilisé par des personnes peu sympathiques ou qui pourraient même vouloir vous harceler ou vous nuire. En surfant sur Internet, vous devez garder à l’esprit certaines règles de base afin de pouvoir vous protéger et protéger les autres

3. Vous avez le droit d’utiliser Internet en toute sécurité et de fixer vos propres limites. Soyez futés, montrez-vous responsables et restez en sécurité quand vous êtes en ligne, tout comme dans la vie réelle!

S COMME SAVOIR FIXER DES LIMITES

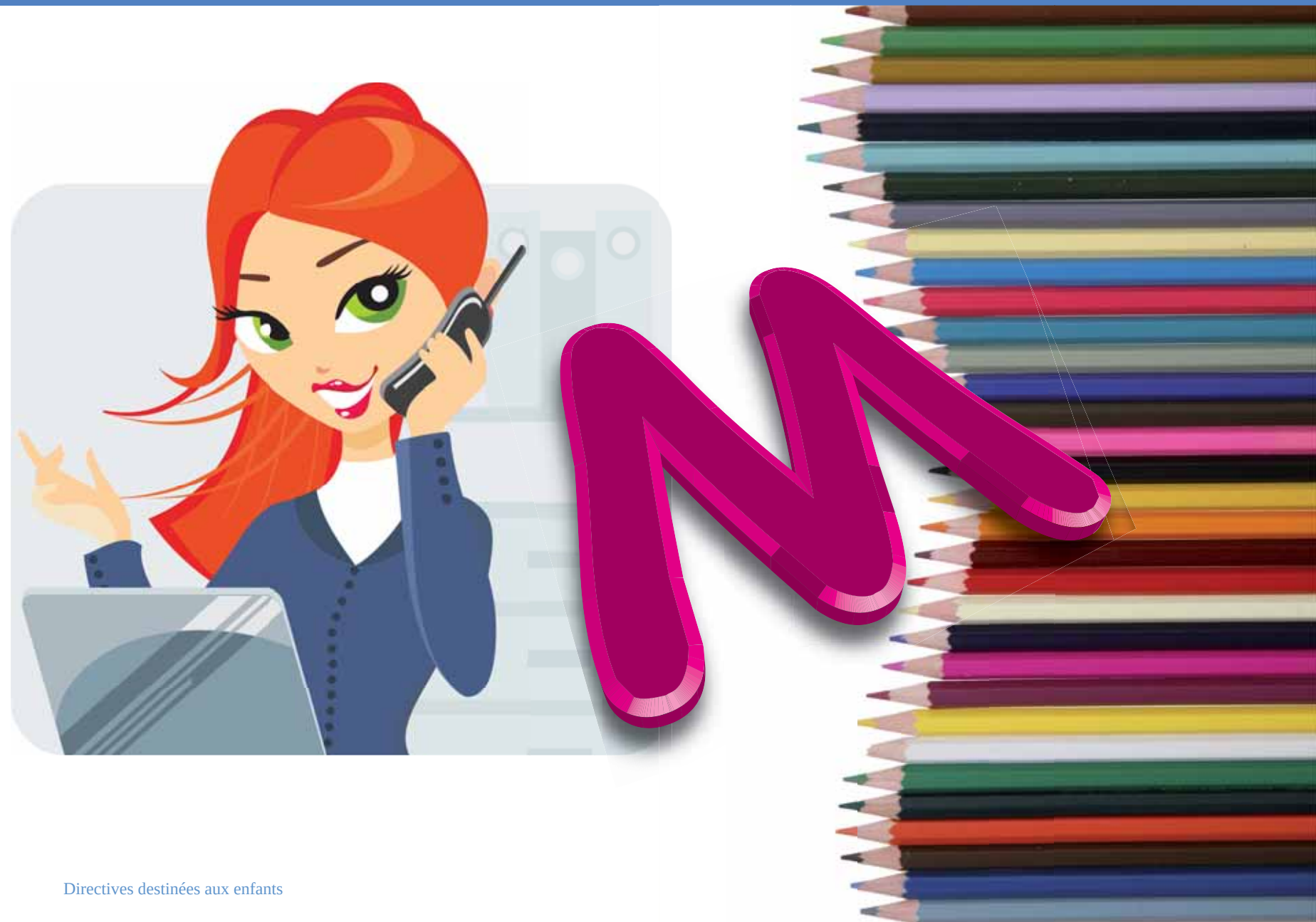
1. Préservez votre sphère privée. Quand vous utilisez un site de réseau social ou tout autre service en ligne, préservez votre sphère privée et celle de votre famille et de vos amis. Il est facile d'avoir le sentiment d'être anonyme quand on est en ligne, mais par la collecte de renseignements provenant de diverses sources, on peut finir par rassembler beaucoup d'informations privées sur vous-mêmes et vos proches, y compris votre famille.

2. Si vous adhérez à un site de réseau social, utilisez les réglages assurant la confidentialité pour protéger votre profil en ligne afin que seuls vos amis puissent le voir. Autant que possible, n'utilisez pas votre véritable nom, mais un pseudo reconnaissable par vos vrais amis. D'autres services interactifs, tels que la messagerie instantanée, offrent également souvent des outils de confidentialité. Utilisez-les.

3. Réfléchissez à deux fois avant de publier ou de partager quoi que ce soit en ligne. Etes-vous prêt a ce que tous les internautes en aient connaissance, vos amis proches aussi bien que des étrangers? Une fois que vous aurez mis en ligne des informations, des photos ou tout autre matériel, il se peut que vous ne soyez plus en mesure de le retirer ou d'en empêcher l'utilisation. On ne peut jamais savoir ou il finira par atterrir.

4. Exercez votre esprit critique: certaines choses présentées comme des faits ne sont peut-être pas vraies du tout. Quand les choses semblent trop belles pour être vraies, c'est hélas souvent parce que c'est le cas. Revérifiez toujours deux fois l'information à partir d'autres sources fiables.

5. Vous avez des droits qui doivent etre respectés, tout comme vous devez respecter les droits des autres. Vous ne devez jamais tolérer d'être harcelé. La loi et les règles d'un comportement décent et acceptable sont valables en ligne aussi bien que dans la vie réelle.


N

M COMME MAÎTRISER LES RENCONTRES DANS LE MONDE RÉEL AVEC DES AMIS EN LIGNE

1. Il arrive que les contacts en ligne se transforment en amitiés.

2. Réfléchissez à deux fois avant de rencontrer dans la réalité une personne avec qui vous avez noué une amitié en ligne. Si vous choisissez de rencontrer cet ami, allez toujours au rendez-vous en compagnie d'une personne de confiance. Vous devez demander d'être accompagné par vos parents ou par un autre adulte en qui vous avez confiance afin d'éviter tout problème si la rencontre s'avère décevante.

3. N'oubliez pas qu'un ami en ligne peut se révéler être une personne tout à fait différente de ce que vous croyiez.

A COMME ACCEPTER DES INVITATIONS/AMITIÉS

1. La plupart des gens avec lesquels vous communiquez en ligne sont probablement déjà vos amis dans la vie réelle. Il est également possible de se connecter aux amis de vos amis. Très souvent, cela peut être amusant, mais en même temps, si vous ne connaissez pas réellement quelqu'un, êtes-vous disposé à le compter parmi vos "amis" et à partager avec cette personne exactement les mêmes informations que celles que vous confiez à vos amis les plus anciens et les plus chers?

2. Les connexions en ligne permettent de se connecter avec de parfaits inconnus. Des étrangers peuvent s'adresser à vous pour vous demander de les inclure dans votre liste de contacts et voir votre profil, mais il n'est pas raisonnable d'accepter de telles demandes. Il n'y a rien de mal à refuser des invitations qui ne vous disent rien. Après tout, le but des réseaux sociaux n'est pas d'obtenir toujours plus de contacts.

R COMME RÉAGIR

1. Protégez-vous contre les contenus susceptibles de vous contrarier ou de vous bouleverser. N'accédez pas en connaissance de cause à de tels sites ou ne partagez pas les liens qui y mènent. Si vous voyez quelque chose qui vous dérange, parlez-en à vos parents ou à quelqu'un en qui vous avez confiance.

2. Ne relevez pas les comportements déplacés et quittez les conversations déplaisantes ou les sites ayant un contenu inapproprié. Comme dans la vie réelle, certaines personnes peuvent, pour une raison ou pour une autre, se comporter de manière agressive, insultante ou provocante envers autrui, ou vouloir partager du contenu nocif. Généralement, il vaut mieux simplement les ignorer, puis les bloquer.

3. Bloquez toute personne qui vous contacte en utilisant des e-mails et des commentaires impolis, importuns ou menaçants. Même si le message vous contrarie et vous met mal à l'aise, sauvegardez-le afin de pouvoir le montrer à un adulte pour obtenir un conseil si nécessaire. Vous n'êtes pas le seul à avoir honte du contenu de certains messages.

4. Soyez toujours sur vos gardes si quelqu'un, en particulier un étranger, veut vous parler de sexe. Souvenez-vous que vous ne pouvez jamais être certain de la véritable identité ou des intentions de cette personne. Contacter un enfant ou un adolescent de manière sexuelle est toujours gravement préoccupant; il faut en parler à un adulte de confiance, afin que vous ou l'adulte en question puissiez le signaler.

5. Si vous avez été attiré ou piégé par quelqu'un et que vous avez accepté des actes sexuels ou la transmission de photos sexuelles de vous-même, parlez-en toujours à un adulte de confiance pour qu'il vous conseille et vous aide. Aucun adulte n'a le droit de demander ce genre de choses à un enfant ou à un adolescent – c'est toujours l'adulte qui est responsable!

T COMME TROUVER QUELQU'UN A QUI CONFIER SES SOUCIS

1. Si vous avez des soucis ou des problèmes en ligne, parlez-en à quelqu'un en qui vous avez confiance. Vos parents ou un autre adulte peuvent vous aider et vous donner de bons conseils sur ce qu'il faut faire. Il n'y a pas de problème sans solution! Vous pouvez également appeler un service d'assistance téléphonique pour enfants[25] disponible dans votre pays.

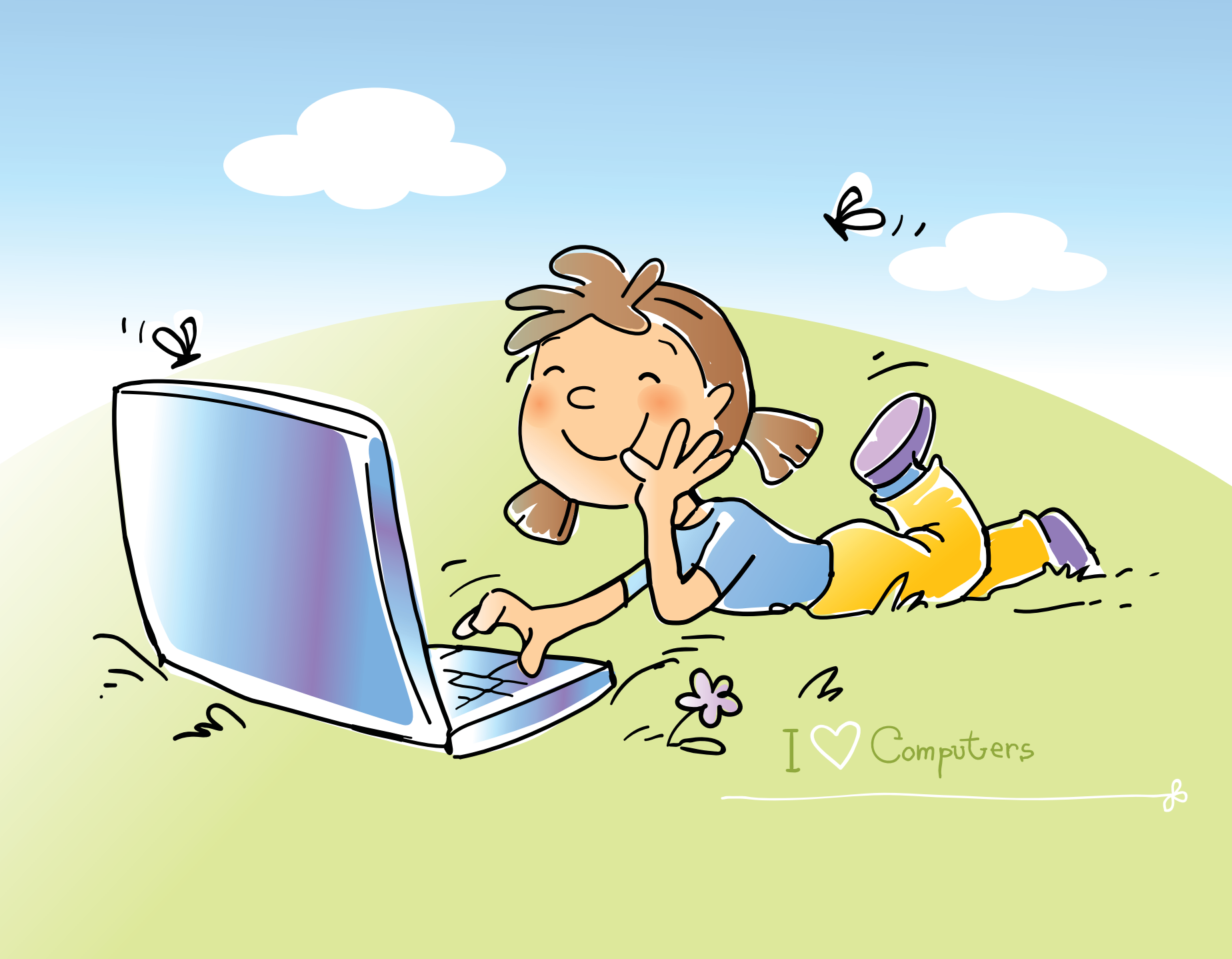
2. Vous pouvez dénoncer les activités ou les contenus nocifs ou inappropriés sur les sites web à l'adresse électronique de l'hôte du site consacrée aux abus.

3. Vous pouvez dénoncer le contenu illégal a une permanence Internet ou à la police.

4. Vous pouvez dénoncer à la police locale les activites illégales ou susceptibles de l'etre.

5. Vous devez vous protéger, mais aussi protéger votre ordinateur ou votre dispositif portable. Comme les règles SMART, il existe quelques conseils aisés a garder en mémoire pour assurer la sécurite de votre ordinateur et de votre mobile.

[25] Par exemple CHI, disponible à www.childhelplineinternational.org


I ♡ Computers

Apprenez à utiliser votre machine en toute sécurité

1. Veillez à installer et à apprendre à utiliser un pare-feu et un logiciel antivirus. N'oubliez pas de les tenir à jour!
2. Apprenez à connaître le système d'exploitation de votre ordinateur (par exemple Windows, Linux, etc.) et en particulier de quelle manière le réparer et le tenir à jour.
3. Si des contrôles parentaux sont installés, parlez-en à vos parents et entendez-vous sur le niveau qui correspond à votre âge et à vos besoins. N'essayez pas de les contourner.
4. Si vous recevez un fichier dont vous n'êtes pas sûr ou dont vous ne connaissez pas l'origine, ne l'ouvrez JAMAIS. C'est par ce biais que votre machine peut être contaminée par un cheval de Troie ou un virus.
5. Apprenez à connaître intuitivement votre machine et la manière dont elle fonctionne afin de réagir si vous détectez quelque chose d'inhabituel.
6. Vérifiez avec qui vous êtes connecté – apprenez à utiliser des outils tels que «Netstat». Enfin, un excellent moyen de garantir que vos parents acceptent de vous voir surfer sur la Toile consiste à signer avec eux un accord écrit. Le but est de les rassurer en montrant que vous connaissez les risques liés au fait d'être en ligne, que vous savez comment vous comporter et quoi faire, ainsi que de faire participer vos parents afin qu'ils sachent ce que vous faites réellement quand vous êtes en ligne. Cet accord doit reposer sur une entente mutuelle entre vous et vos parents. Un exemple d'un tel contrat est donné à la fin des présentes directives (Annexe 1). Vous pourrez trouver en ligne sur Internet différentes versions d'un contrat familial sur la sécurité.

Vos droits en ligne

- Vous avez le droit de faire usage des technologies pour développer votre personnalité et vos capacités;
- Vous avez le droit de protéger votre identité;
- Vous avez le droit de participer, de vous amuser et d'accéder à des informations adaptées à votre âge et à votre personnalité;
- Vous avez le droit de vous exprimer librement et d'être traité avec respect tout en respectant toujours les autres;
- Vous avez le droit de critiquer et de discuter tout ce que vous lisez ou rencontrez en ligne;
- Vous avez le droit de dire NON si quelqu'un vous demande quelque chose qui vous met mal à l'aise quand vous êtes en ligne.

Directives pour la tranche d'âge de 5 à 7 ans

De nombreux enfants de cet âge ne sont pas capables de lire ou de comprendre des directives telles que celles-ci. En outre, l'utilisation qu'ils font d'Internet devrait être étroitement surveillée à tout moment par un parent ou un adulte. Les logiciels de filtrage et autres mesures techniques peuvent également jouer un rôle particulièrement utile pour soutenir l'utilisation d'Internet par un enfant de cet âge. Il est judicieux de restreindre les possibilités d'accès à Internet d'un jeune de cet âge, par exemple en établissant une liste de sites web sûrs qui sont adaptés à son âge. Le but est d'inculquer à ce groupe les règles fondamentales de la sécurité sur Internet, de l'étiquette et de la compréhension. Cette tranche d'âge ne sera sans doute pas en mesure de décoder des messages plus sophistiqués. Les parents ou les adultes responsables de l'enfant devraient consulter les directives COP destinées aux parents, aux tuteurs et aux éducateurs afin de voir comment aider au mieux le groupe des plus jeunes à surfer en toute sécurité. Par ailleurs, plusieurs liens utiles et intéressants menant à des ressources en ligne pour cette tranche d'âge sont indiqués à la section «Lectures recommandées et autres sources d'inspiration».

Directives pour la tranche d'âge de 8 à 12 ans

On peut faire des tas de choses différentes en ligne. Le plus souvent, c'est très amusant, mais parfois cela ne se passe pas aussi bien qu'on l'espérait, sans que l'on sache tout de suite pourquoi, ni comment y réagir. Cette section contient quelques conseils vraiment utiles pour vous aider à surfer en toute sécurité.

Bavarder avec des amis en utilisant la messagerie instantanée, en participant à des *chat rooms* ou en allant sur des sites de réseau social peut être formidable pour se tenir au courant de tout. Il est également amusant de se faire de nouveaux amis en ligne. Sur Internet, vous pouvez rencontrer des gens qui aiment les mêmes films ou les mêmes sports que vous.

Mais s'il est vrai qu'il y a beaucoup d'avantages à garder le contact avec ses amis en ligne, il existe aussi des risques à rencontrer des gens en ligne – surtout si on ne les connaît pas dans la vie réelle.

Pour rester en sécurité tout en bavardant en ligne, n'oubliez pas quelques conseils simples:

1. Soyez vigilants en ce qui concerne les personnes en qui vous faites confiance en ligne. On peut faire semblant d'être quelqu'un que l'on n'est pas.
2. Choisissez vos amis. Certes, il est agréable d'avoir beaucoup d'amis, mais si vous en avez trop, vous aurez du mal à contrôler qui peut voir ce que vous postez en ligne. N'acceptez pas les demandes d'amitiés venant de personnes que vous ne connaissez pas réellement et dont vous n'êtes pas sûr.
3. Gardez la confidentialité sur vos détails personnels. Utilisez un pseudo au lieu de votre vrai nom si vous êtes sur un site ou dans un jeu rassemblant beaucoup de personnes inconnues. Demandez à vos parents avant de donner votre nom, votre adresse, votre numéro de téléphone ou tout autre détail privé à quiconque sur Internet.
4. Réglez votre profil sur «confidentiel». Demandez à vos parents de vous aider. Ne le faites pas si vous n'êtes pas sûr. C'est vraiment important.
5. Conservez toujours votre mot de passe secret. Ne le communiquez pas, même à vos amis.
6. Si vous voulez organiser un rendez-vous avez quelqu'un que vous avez rencontré en ligne, parlez-en d'abord avec vos parents, et demandez que l'on vous accompagne. La rencontre doit toujours avoir lieu dans un endroit public largement éclairé, en présence de beaucoup de monde, de préférence pendant la journée.
7. Si quelqu'un écrit quelque chose d'impoli, d'inquiétant ou qui vous déplaît, parlez-en à vos parents ou à un autre adulte en qui vous avez confiance.

Netiquette

Parfois il est facile d'oublier que la personne avec laquelle on discute sur messagerie instantanée, avec laquelle on joue ou sur le profil de laquelle on poste un commentaire est un individu en chair et en os. En ligne, il s'avère plus facile de dire ou de faire des choses que l'on ne ferait peut-être pas dans la «vie réelle». On peut ainsi vexer les gens, les mettre mal à l'aise ou leur donner un sentiment d'insécurité. Il est important d'être aimable et poli envers les autres sur Internet – pensez à la manière dont ils seront affectés par votre comportement.

Conseils

Traitez les autres comme vous voudriez qu'ils vous traitent. Evitez d'utiliser des termes impolis et ne dites rien qui puisse mettre les autres mal à l'aise.

Apprenez la «netiquette», c'est-à-dire les règles de comportement en ligne. Qu'est-ce qui est considéré comme approprié ou non? Par exemple, si vous tapez un message en LETTRES MAJUSCULES, votre interlocuteur pourra croire que vous êtes en train de crier.

Si quelqu'un dit quelque chose d'impoli ou qui vous met mal à l'aise, ne répondez pas. Quittez le *chat room* ou le forum sans attendre.

Si vous lisez un texte qui vous contrarie, que vous voyez une image obscène ou quelque chose qui vous effraie, parlez-en à vos parents ou à un autre adulte de confiance.

Jeux en ligne

On peut avoir beaucoup de plaisir à jouer en ligne ou à utiliser des consoles ou des jeux sur ordinateur, mais il faut être vigilant quant à la durée du jeu et aux personnes avec qui on joue. Si vous bavardez avec d'autres joueurs, il est important que vous protégiez votre sphère privée et ne communiquiez aucune information personnelle ou privée. Si vous n'êtes pas certain qu'un jeu soit approprié, demandez à vos parents ou à un adulte de confiance de contrôler sa classification et ses critiques pour vous.

Conseils

1. Si un autre joueur se comporte mal ou vous met mal à l'aise, bloquez-le de votre liste de joueurs. Vous pouvez aussi le dénoncer à l'opérateur du site de jeux.
2. Limitez votre temps de jeu afin d'avoir encore la possibilité d'autres activités telles que faire vos devoirs, accomplir des tâches domestiques ou passer du temps avec vos amis.
3. Gardez la confidentialité sur vos détails personnels.
4. N'oubliez pas de passer du temps hors connexion avec vos amis, à pratiquer vos sports favoris et à entreprendre d'autres activités.

Harcèlement

Les règles applicables en ligne à la manière de traiter les autres sont les mêmes que dans la «vie réelle». Malheureusement, les gens ne se traitent pas toujours bien en ligne et vous pouvez (vous ou un de vos amis) être la cible de harcèlement et de brimades. Il est possible que l'on vous taquine ou que l'on répande sur Internet des rumeurs sur votre compte, que l'on vous envoie des messages obscènes ou même des menaces. Cela peut se passer à l'école, ou en dehors, à n'importe quelle heure de la journée, et émaner de personnes que vous connaissez ou même de parfaits inconnus. Une telle expérience peut vous déstabiliser et vous donner un sentiment d'isolement.

Personne n'a le droit de harceler quiconque. Dans sa forme la plus extrême, le harcèlement est illégal et peut faire l'objet d'une enquête par la police.

Conseils

Si on vous harcèle en ligne:

1. N'en tenez pas compte. Ne répondez pas à l'agresseur. S'il ne reçoit pas de réponse, il se lassera et s'en ira.
2. Bloquez cette personne. Cela stoppera l'arrivée des messages ou des textes venant de cette personne en particulier.
3. arlez-en à quelqu'un, à vos parents ou à un autre adulte en qui vous avez confiance. Gardez les traces. Cela peut être utile pour repérer l'auteur du harcèlement. Sauvegardez les textes, les courriers

électroniques, les conversations en ligne ou les messages vocaux afin qu'ils servent de preuves.

4. Dénoncez-le:

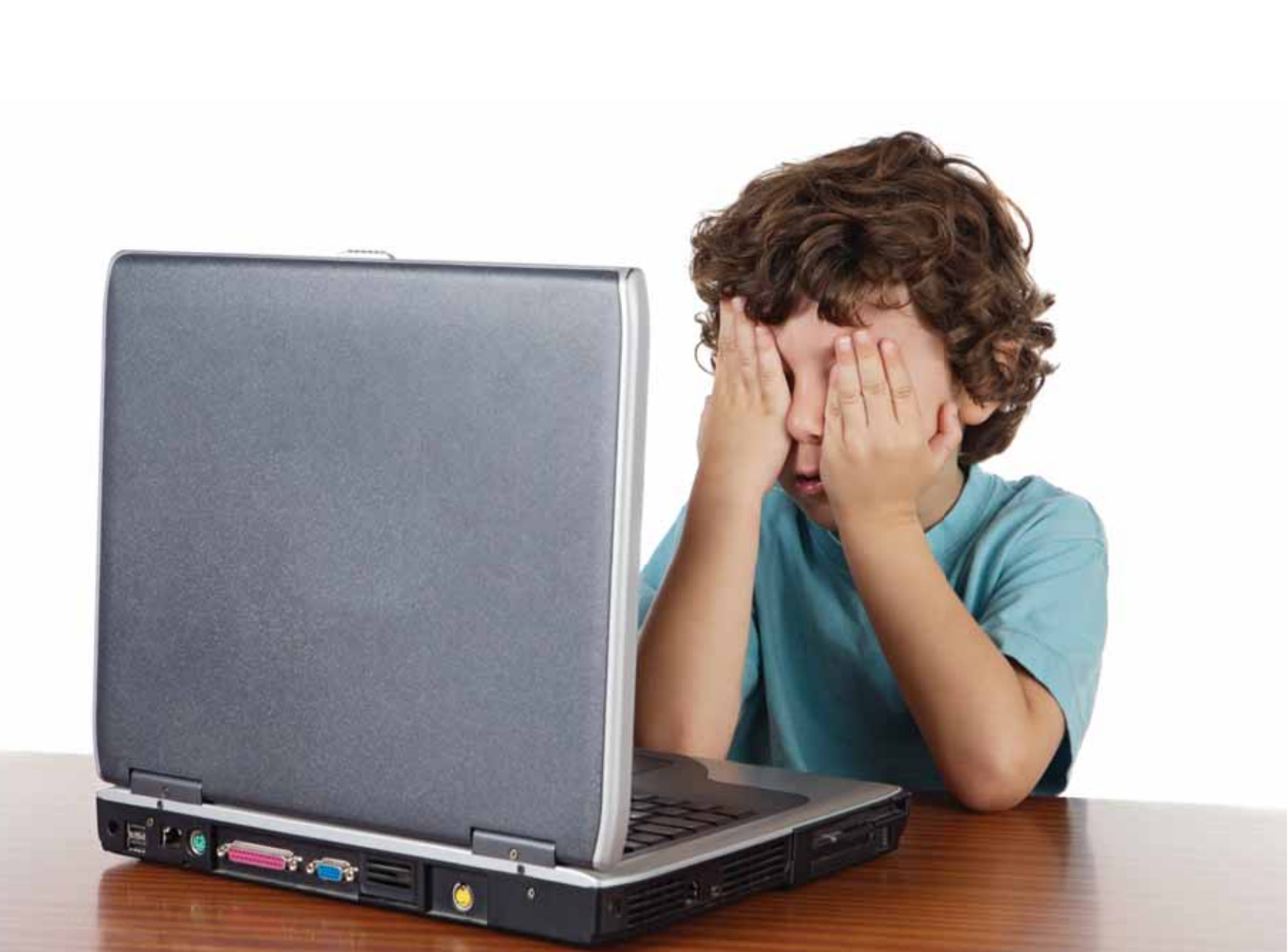
- dans votre école – celle-ci devrait avoir une politique pour lutter contre l'intimidation.
- auprès de votre fournisseur de service Internet et / ou fournisseur téléphonique ou administrateur du site – il y a des mesures qu'ils peuvent prendre pour vous aider.
- à la police – si votre sécurité est menacée, la police vous aidera.

Si un ami est victime de harcèlement en ligne

Il peut s'avérer difficile de savoir si vos amis sont victimes de brimades. Ils le gardent peut-être pour eux-mêmes. En cas de harcèlement, vous remarquerez peut-être que vos amis ne bavardent pas aussi souvent en ligne, ou bien reçoivent tout à coup beaucoup de messages SMS, ou sont tristes après avoir consulté leur ordinateur ou écouté leurs messages vocaux. Il peut leur arriver de se couper de leurs amis ou de se désintéresser de l'école ou des activités sociales.

Aidez à mettre fin au harcèlement

1. Ne vous laissez pas faire et parlez-en ouvertement! Si vous constatez ou que vous apprenez qu'un ami est victime de brimades, apportez-lui votre soutien en dénonçant le harcèlement. C'est ce que vous voudriez qu'il fasse si cela vous arrivait.
2. Ne transférez pas de messages ou d'images susceptibles de vexer ou de choquer quelqu'un. Même si ce n'est peut-être pas vous qui avez commencé, vous serez considéré comme complice de harcèlement.



3. N’oubliez pas de traiter les autres comme vous voudriez qu’ils vous traitent lorsque vous communiquez en ligne.

Votre empreinte numérique

Il est formidable de pouvoir échanger en ligne avec ses amis. Une partie du plaisir que l’on a à partager des vidéos, des photos et d’autres contenus tient à ce qu’un grand nombre de personnes peuvent les voir et y réagir. N’oubliez pas que ce que vous partagez avec vos amis peut être aussi visualisé par des inconnus. Parfois, ils peuvent même continuer à le consulter pendant encore des années. Tout ce que vous mettez en ligne s’ajoute à votre empreinte numérique et pourrait bien rester en ligne pour toujours. Il vaut donc mieux réfléchir avant de poster quelque chose

Conseils

1. Gardez la confidentialité sur vos détails personnels. Utilisez un pseudo approprié plutôt que votre vrai nom. Demandez à vos parents avant de donner à quiconque sur Internet votre nom, votre adresse, votre numéro de téléphone ou tout autre détail personnel.
2. Ne communiquez à personne votre nom d’utilisateur ou votre mot de passe.
3. Réfléchissez avant d’appuyer sur la touche d’envoi ou de mise en ligne. Une fois posté, le contenu pourrait s’avérer difficile à retirer.
4. Ne postez pas ce que vous ne voulez pas que les autres sachent ou découvrent – ou ce que vous ne leur diriez pas de vive voix.
5. Souvenez-vous que les images et vidéos privées que vous envoyez à des amis ou que vous postez sur un site de réseau social peuvent être transmises à d’autres et ensuite mises sur des sites publics.
6. Soyez respectueux du contenu d’autrui que vous postez ou que vous partagez. Ainsi, la photo qu’un de vos amis a prise lui appartient à lui, et non à vous. Vous ne devez la mettre en ligne que si vous avez obtenu sa permission et si vous veillez à mentionner de qui vous l’avez obtenue.

Contenu déplacé ou illégal

En surfant sur le web, on peut rencontrer des sites web, des photos, des textes ou d’autres matériels qui mettent mal à l’aise ou qui choquent. Il existe quelques conseils faciles à suivre pour gérer ce genre de situations.

Conseils

1. Si vous rencontrez quelque chose qui vous choque, parlez-en à vos parents ou à un autre adulte de confiance.
2. Sachez comment «échapper» à un site web si une recherche sur Internet vous amène à un site déplaisant ou obscène. Appuyez sur control-alt-delete si le site ne vous autorise pas à le quitter.
3. Si un site web vous paraît suspect ou comporte une page d’avertissement pour les jeunes de moins de 18 ans, quittez-le immédiatement. Certains sites ne sont pas destinés aux enfants.
4. Vérifiez avec vos parents que votre moteur de recherche est réglé pour bloquer le matériel destiné aux adultes.
5. Demandez à vos parents d’installer des logiciels de filtrage Internet afin de bloquer les sites inappropriés.
6. Demandez à vos parents de vous aider à trouver des sites sûrs et amusants et mettez-les dans vos signets pour plus tard.

Tranche d'âge des plus de 13 ans

Un nombre considérable de jeunes appartenant à cette tranche d'âge utilise des sites de réseau social, des jeux en ligne et des applications de messagerie instantanée. Ils ne vont pas simplement sur Internet de manière occasionnelle ou pour le plaisir. Pour beaucoup d'entre eux, cela fait partie intégrante de leur vie quotidienne. C'est par ce biais qu'ils restent en contact avec leurs amis et communiquent avec eux, qu'ils organisent une large part de leur vie sociale et de leur travail à l'école. Voici quelques informations sur la manière d'utiliser ces plates-formes en ligne en toute sécurité ainsi qu'un aperçu de ce que l'on peut faire pour contribuer à créer un espace en ligne positif et sans danger.

Contenu nocif et illégal

Internet est un excellent outil pour satisfaire des besoins tels que la curiosité, l'intérêt ou le désir d'apprendre et d'expliquer de nouvelles facettes du savoir. Mais Internet est un monde ouvert où chacun est libre de diffuser ce qu'il veut. Il contient une quantité infinie d'informations, d'une portée si vaste qu'il est facile de s'y perdre ou de rencontrer des contre-vérités ou du matériel inadapté à vos besoins ou à votre âge. Nous pensons aux sites qui, par exemple, encouragent la haine raciale ou incitent à la violence, ou qui sont susceptibles de vous exposer à du matériel pornographique ou constituant des mauvais traitements envers les enfants. Cela peut survenir de façon totalement accidentelle, lors de recherches sur des sujets totalement différents, par le biais de courriers électroniques, de programmes P2P, de forums, de *chat rooms* et, plus généralement, par le biais de nombreux canaux impliqués dans les réseaux sociaux.

C'est pourquoi:

1. Avant d'entamer une recherche, il faut avoir une idée claire de ce que l'on cherche.
2. Pour limiter la recherche, vous pouvez utiliser des fonctions de recherche avancées ou des répertoires, c'est-à-dire des catégories thématiques, assurées par la plupart des moteurs de recherche (par exemple sports, santé, cinéma, etc.).
3. Faites preuve d'esprit critique et essayez de déterminer si le site est digne de confiance; lorsque vous y accédez, est-ce que d'autres pages commencent à s'ouvrir automatiquement? Etes-vous en mesure de découvrir le propriétaire du site? Est-il facile de le contacter? Pouvez-vous dire qui est l'auteur de la page ou de l'article particulier que vous êtes en train de regarder? (Il est toujours possible de faire une autre recherche pour en apprendre davantage sur l'auteur et/ou le propriétaire). Assurez-vous de n'avoir pas fait de faute de frappe en tapant l'adresse du site; certains sites utilisent un nom qui ressemble à un autre afin de profiter d'éventuelles erreurs de dactylographie. Le texte du site est-il correctement épelé ou bien y a-t-il des erreurs de grammaire?Est-ce qu'il comporte des dates permettant d'indiquer sa dernière actualisation?Y a-t-il des mentions légales (concernant, par exemple, le respect de la sphère privée)?
4. Si, en surfant, vous tombez sur des sites contenant du matériel violent, raciste, illégal ou bien où des enfants sont maltraités, n'oubliez pas que ces sites peuvent être dénoncés à la police ou à une permanence téléphonique.

Essayez de découvrir à qui il est possible de soumettre ces plaintes dans votre pays; vos parents ou un autre adulte de confiance peuvent également vous aider à porter plainte. Il serait également bon de parler à quelqu'un de ce qui s'est passé et de tout sentiment qui pourrait encore vous agiter suite à cet incident ou cette expérience.

5. Les contenus (images, vidéos, etc.) à caractère sexuel qui se trouvent sur le web peuvent souvent être de nature pornographique et transmettre du matériel sexuel d'une manière propre aux adultes, avec des sentiments qui ne sont pas appropriés pour votre tranche d'âge.

Qu'est-ce que le *grooming*?

Il peut arriver qu'Internet ou les téléphones portables soient utilisés de manière abusive par des adultes qui veulent entrer en contact avec des jeunes garçons ou des jeunes filles. Cela passe en particulier par des messages SMS et MMS, des *chat rooms*, des messages instantanés, des forums de discussion, des jeux en ligne ou, plus généralement, par tous les espaces de réseau social où il est possible d'obtenir des informations sur l'âge, le sexe des utilisateurs et davantage encore, par le biais des profils qu'ils ont établis.

Des prédateurs sexuels recourent à Internet pour contacter des enfants et des adolescents à des fins sexuelles, souvent à l'aide d'une technique de manipulation psychologique appelée «*grooming*». Cette technique consiste à gagner la confiance de l'enfant ou de l'adolescent en faisant appel à ses centres d'intérêts. Ces prédateurs sont extrêmement manipulateurs. Ils évoquent souvent des sujets de nature sexuelle, utilisent des photos et des termes explicites pour sensibiliser aux questions sexuelles et faire en sorte que leurs victimes visées baissent la garde. Ils remettent parfois à l'enfant des cadeaux, de l'argent et même des titres de transport afin de l'attirer à un endroit où le prédateur pourra l'exploiter sexuellement. Ces rencontres peuvent même être photographiées ou filmées sur vidéo; si la rencontre n'a pas lieu dans le monde réel, le prédateur peut aussi convaincre l'enfant de prendre des photos sexuelles de lui ou de ses amis ou de participer à des activités sexuelles en recourant à une webcam pour les diffuser. De nombreux enfants et adolescents qui se retrouvent impliqués dans ce genre de relations avec un prédateur manquent légèrement de maturité émotionnelle ou ont une faible estime de soi. Cela peut les rendre vulnérables à ce genre de manipulation et d'intimidation. Ils peuvent également se montrer réticents à parler de leurs rencontres à des adultes, par crainte d'être gênés ou de perdre le droit d'accéder à Internet. Dans certains cas, ils subissent des menaces de la part des prédateurs qui les incitent à ne rien dire de leur relation ou de ce qui s'est passé.

C'est la raison pour laquelle:

1. Il est essentiel d'être au courant de ce risque, et du fait que tous les internautes ne sont pas nécessairement qui ils prétendent être. Les séducteurs en ligne peuvent souvent prétendre avoir votre âge afin de créer une atmosphère de familiarité et de confiance susceptible d'aboutir à une rencontre hors ligne et éventuellement à un abus.
2. Il est important de protéger ses données personnelles; dans le monde réel, vous ne donneriez jamais ce genre de détails et vous ne raconteriez jamais des choses privées à des gens que vous ne connaissez pas. Même si vous avez noué une belle amitié virtuelle qui donne l'impression qu'elle pourrait aboutir à plus, vous ne devez pas oublier que vous


http://Bullying...

ne savez pas toujours qui est réellement à l'autre bout de l'ordinateur.

3. Pour entrer dans un chat room, un forum ou plus généralement un réseau social, il faut souvent compiler un profil personnel, en donnant des informations qui peuvent être plus ou moins détaillées. Dans de tels cas, il est essentiel d'être prudent avant de fournir des données identifiables ou traçables (nom et prénom, adresse, nom de votre école, numéro de téléphone portable, adresse électronique, etc.). Ce genre de détails peut finir par tomber entre les mains de n'importe qui; il vous est donc conseillé de vous créer une identité, en utilisant un pseudo ou un surnom ainsi que des images fictives ou avatars, et de ne pas fournir d'informations personnelles détaillées.
4. Si vous éprouvez de la curiosité sur votre sexualité ou vos sentiments plus intimes, souvenez-vous qu'Internet peut parfois être une source de bons conseils et d'informations utiles, mais que très souvent, il vaut mieux essayer de trouver un moyen de discuter de ces choses avec des gens que vous connaissez déjà et en qui vous avez confiance dans la vie réelle.
5. Si quelqu'un tente de vous séduire ou s'il se produit une situation embarrassante, il est important que vous trouviez un adulte ou un ami à qui en parler; de même, les fournisseurs de service Internet permettent souvent aux utilisateurs de signaler des incidents en cliquant sur «report» ou «notify», afin de dénoncer l'abus. Vous pouvez aussi vous adresser directement à la police.

Il est également recommandé de sauvegarder les courriers électroniques et les textes de chat rooms, les messages SMS ou MMS (en utilisant par exemple la boîte «messages arrivés»), parce qu'ils peuvent être transmis comme preuves à la police.

Harcèlement

Les services tels que le courrier électronique, les forums, les *chat rooms*, les blogs, les programmes de messagerie instantanée, les SMS et MMS, et les caméras vidéo permettent de garder le contact avec de vieux amis ou de s'en faire de nouveaux en temps réel et dans toutes les régions du monde, ainsi que d'échanger des idées, de jouer, de faire des recherches, etc. Il est vrai que la plupart de ces services et les manières dont on s'en sert sont utiles, mais dans certains cas, ces mêmes outils peuvent servir à choquer les internautes, se moquer d'eux, les diffamer ou plus généralement les embêter; de plus, des comportements violents ou offensants dans le monde réel se trouvent amplifiés lorsqu'ils sont filmés sur des téléphones portables et échangés ou postés sur la Toile.

Qu'est-ce que le harcèlement? Harceler, c'est faire intentionnellement du mal à quelqu'un en le rudoyant oralement, en l'agressant physiquement ou en appliquant d'autres méthodes de contrainte plus subtiles telles que la manipulation. Dans la langue de tous les jours, on parle souvent de harcèlement, brimades ou intimidation pour décrire l'abus de pouvoir commis par quelqu'un qui est physiquement plus fort que sa victime ou qui possède une position sociale dominante. La victime du harcèlement est souvent appelée cible. Le harcèlement peut être verbal, physique et/ou émotionnel (www.wikipedia.org).

Très souvent, le harcèlement se produit à l'école ou non loin de chez soi. Malheureusement, les agresseurs sont de plus en plus nombreux, tout comme les

formes réelles de harcèlement en ligne, qui vont des sites web déplacés jusqu'à l'intimidation par textos, en passant par l'envoi de photos non souhaitées par le biais de téléphones portables, et ainsi de suite. Cette forme particulière de harcèlement – qui peut éventuellement vexer et blesser quelqu'un sans nécessairement impliquer un contact physique – peut avoir des conséquences tout aussi douloureuses que les formes de harcèlement traditionnelles.

C'est la raison pour laquelle il est important de connaître l'existence de ce phénomène, d'être au courant des différentes formes qu'il peut prendre et de savoir ce qu'il est possible de faire pour éviter de devenir une victime:

1. Ne diffusez pas vos données personnelles de manière irréfléchie, car cela pourrait vous rendre aisément identifiable et plus vulnérable à des actes de harcèlement et d'intimidation de la part d'autres personnes de votre âge.
2. Une fois que l'information est mise en ligne, elle échappe à votre contrôle; elle devient disponible pour n'importe qui et ouverte à toutes sortes d'utilisations. Il faut en être parfaitement conscient; ce qui peut sembler être une blague innocente pourrait avoir des conséquences très irritantes et dommageables pour d'autres.
3. Il est important de s'abstenir de réagir à des provocations reçues par SMS, MMS, messages instantanés, courriels agressifs ou diffamatoires, dans des *chat rooms* ou lors de rencontres en ligne avec d'autres utilisateurs. Au lieu de réagir, vous devez employer certaines stratégies capables d'exclure ceux qui tentent de vous provoquer ou de limiter leurs possibilités d'agir, par exemple:
   - de nombreux jeux permettent d'exclure les utilisateurs indésirables (ou non souhaités);
   - lorsque des chat rooms sont surveillés, il est possible de sauvegarder le texte choquant afin de le signaler au surveillant;
   - les abus peuvent être dénoncés aux fournisseurs de services ou, dans le cas d'abus par téléphone portable, en envoyant un rapport à la société de téléphonie mobile;
   - dans les cas plus graves, tels que ceux impliquant des menaces physiques, il est conseillé d'informer également la police;
   - il est possible de retrouver le compte de courrier électronique à partir duquel le message choquant a été envoyé, mais pratiquement impossible de prouver qui l'a effectivement utilisé pour envoyer le message. L'auteur du harcèlement en ligne peut également pénétrer par piratage dans le compte de quelqu'un d'autre et l'utiliser pour se montrer agressif, ce qui fait ainsi porter le chapeau au malheureux dont le compte électronique a été détourné;
   - la plupart des programmes de courrier électronique offrent des filtres pour bloquer l'arrivée de courriers électroniques non souhaités.
4. De nombreux programmes de messagerie instantanée offrent la possibilité de créer une liste de noms que les utilisateurs peuvent choisir de bloquer. De cette manière, vous pouvez empêcher les indésirables d'entrer en contact avec vous. Un système de messagerie instantanée vous fait savoir quand un de vos contacts connus et approuvés est en ligne et, à partir de là, vous pouvez commencer à bavarder avec la personne avec laquelle vous avez envie de parler.

Il existe un certain nombre de systèmes de messagerie instantanée différents, tels que ICQ, AOL Messenger, Yahoo Messenger! Les auteurs de harcèlement savent quels sont les plus populaires parmi les jeunes, et y recourent à leurs propres fins, telles que la violence ou le fait de provoquer une bagarre en ligne. Les conversations ou les bagarres qui surviennent peuvent parfois se prolonger à l'école ou ailleurs dans le monde réel.

Dans tous les cas, n'oubliez pas qu'il est important de parler à quelqu'un de ce qui se passe s'il vous arrive de vous sentir mal à l'aise ou d'être menacé.

Dites-le à vos parents, à un enseignant ou à un employé de l'école en qui vous pouvez avoir confiance. Même le fait d'en parler à vos amis peut être utile.

Vous pouvez également le signaler au fournisseur de service ou à l'opérateur mobile, et même à la police dans les cas graves. N'oubliez pas de sauvegarder les preuves du harcèlement, car elles auront réellement de l'importance lorsque vous en parlerez à quelqu'un.

Le harcèlement n'est pas acceptable, ni dans un environnement en ligne ni dans le monde réel.

Dans de nombreux pays, il existe des organismes nationaux ou locaux auxquels on peut s'adresser pour obtenir de l'aide.

Dans certains pays tels que le Canada, la «cyberintimidation» est considéré comme un véritable délit. Dans la plupart des pays, menacer quelqu'un, le harceler ou le traquer, tant dans la vie réelle que sur Internet, constitue un délit pénal.

Notons au passage que le terme anglais de «bully» qui désigne l'agresseur avait initialement une signification très différente de celle d'aujourd'hui – en fait, il y a 500 ans, il signifiait «ami» ou «membre de la famille» – les choses ont bien changé!

Protégez votre sphère privée

De nos jours, il est relativement simple de créer un blog ou un site web personnel. Pour adhérer à un *chat room*, un forum ou plus généralement un réseau social, il faut d'abord créer un profil personnel qui comporte des types d'informations plus ou moins détaillés. Tous les sites n'ont pas les mêmes règles. Avant d'entrer la moindre information vous concernant dans la base de données d'un site ou les dossiers des membres, vérifiez de quelle manière cette information peut être utilisée, si elle sera publiée en tout ou en partie et si oui, où. Si vous êtes dérangé par la quantité d'information que l'on vous demande, si vous ne connaissez pas vraiment le site ou si vous ne lui faites pas confiance, ne répondez pas. Cherchez un autre service ou un service similaire qui demande moins d'informations ou qui promet de traiter vos informations avec plus de soins. Dans toute la mesure du possible, il est recommandé de créer une identité (ou pseudo) en utilisant un surnom inventé sans rien y ajouter. Surtout, il est important de comprendre clairement ce qui peut finir par être divulgué et ce qu'il vaut mieux ne pas partager avec d'autres. Ce qui est mis en ligne peut rapidement échapper à votre contrôle et se retrouver à la disposition de n'importe qui pour n'importe quel usage:

1. Chaque fois que vous devez communiquer vos données personnelles, assurez-vous que la personne qui vous les demande est authentique et sérieuse, et n'oubliez pas non plus qu'avant de transmettre des données relatives à vos amis, vous devez d'abord les en informer et obtenir leur permission, parce qu'il se pourrait qu'ils ne soient

Directives destinées aux enfants

pas ravis de voir leur adresse électronique ou d'autres informations les concernant être transmises à des tiers;

2. Il peut arriver que vous ne soyez pas obligé de fournir toutes les informations qui vous sont demandées; il est alors recommandé de n'insérer que les types de données qui sont strictement requises. En tout état de cause, il est toujours conseillé de se procurer autant de renseignements que possible sur la personne, le service ou l'entreprise avec laquelle on a affaire, avant de communiquer ses données. En particulier, vérifiez si le site qui demande des données se propose de vous envoyer du matériel publicitaire, ou envisage de transmettre vos données personnelles à d'autres sociétés. Si vous n'êtes pas d'accord, cochez les cases correspondantes. Si ce site ne vous donne pas le choix, peut-être devriez-vous plutôt envisager de ne pas utiliser du tout ce service.
3. N'envoyez des photos et des vidéos personnelles qu'aux personnes que vous connaissez réellement; votre image fait partie de vos données personnelles, et vous devez vous assurer qu'elle n'est pas diffusée à la légère. Il en va de même pour les photos des autres. N'oubliez pas qu'il est pratiquement impossible de déterminer où une photo en ligne peut finir par se retrouver; avant de filmer ou de photographier quelqu'un, vous devez toujours lui demander la permission.
4. Lorsque vous devez vous inscrire à un service particulier, employez quelques astuces simples: par exemple, choisissez un mot de passe difficile à deviner, afin que personne ne puisse le découvrir pour accéder à votre compte; utilisez une adresse électronique complexe, si possible avec des chiffres et des lettres (par exemple mrx-3wec97@... .com) afin qu'elle devienne plus difficile à percer à jour par les spammeurs ou les inconnus qui pourraient vouloir vous envoyer des courriers non désirés; assurez-vous que votre service anti-spam (pour les mails arrivant) et les contrôles anti-virus (pour les pièces jointes) soient activés et continuellement actualisés; utilisez deux adresses électroniques, une qui restera strictement personnelle et uniquement destinée à la correspondance avec vos contacts de la vie réelle (amis, parents, etc.), et l'autre qui sera inscrite dans tous les formulaires d'enregistrement en ligne qui réclament des données personnelles (profils d'utilisateurs, annonces de concours, jeux en ligne, etc.), parce que vous savez déjà qu'elle pourrait être obtenue par des étrangers.
5. N'ouvrez pas de pièces jointes venant de sources inconnues, ni de programmes dont vous ignorez les effets possibles, il pourrait s'agir d'un «*key logger*» (capable d'enregistrer toutes les touches actionnées sur le clavier, ce qui permet de découvrir les mots de passe, les codes numériques, les numéros de cartes de crédit, etc.), d'un «*e-grabber*» (capable d'accéder à toutes les adresses électroniques enregistrées sur le PC de la victime), ou d'un «info grabber» (capable d'extraire des informations telles que les diverses touches d'enregistrement des plus importants programmes sur un PC). A votre insu, ces programmes peuvent envoyer sur Internet à des inconnus toutes les informations qu'ils captent.
6. N'entreprenez que les activités dont vous avez le sentiment qu'elles sont totalement sûres. Si vous pensez qu'il y

a «anguille sous roche», que quelque chose n'est pas tout à fait correct, si vous n'êtes pas totalement convaincu ou si vous pensez qu'on vous demande un prix disproportionné pour quelque chose, la meilleure solution consiste à abandonner cette activité. Vous avez le droit de critiquer et de remettre en question ce que vous rencontrez quand vous êtes en ligne. N'oubliez pas que les choses ne sont pas toujours ce qu'elles semblent être.

Respectez le droit d'auteur

Ce qu'il y a de formidable avec le web, c'est l'infinité des possibilités qui existent pour trouver toutes sortes de matériels grâce à des moteurs de recherche, et pour les télécharger ensuite gratuitement ou en payant par le biais du PC ou du téléphone portable, afin de les utiliser ensuite hors ligne.

Tout ce que l'on trouve en ligne n'est pas nécessairement utilisable à volonté; beaucoup de contenu est protégé par la législation sur le *copyright* ou couvert par certains droits.

Les logiciels Peer-to-Peer (P2P) permettent de partager et d'échanger ses fichiers directement avec d'autres internautes, sans coûts de connexion supplémentaires. Musique, films, vidéos et jeux figurent parmi les matériels les plus recherchés et les plus téléchargés par les jeunes, mais ils sont souvent couverts par les dispositions du droit d'auteur et protégés par la loi. Le téléchargement et la distribution non autorisés de contenu protégé par le droit d'auteur sont des délits réprimés par la loi dans la plupart des pays. Il est également possible de remonter jusqu'à vous si vous avez participé au téléchargement illégal de matériel couvert par le droit d'auteur. Il est ainsi arrivé que les parents d'un enfant reçoivent une énorme facture pour couvrir le coût du matériel téléchargé; si la famille refuse de payer la facture, elle est passible d'autres poursuites juridiques. Certains pays envisagent d'interdire l'utilisation d'Internet aux personnes qui sont régulièrement détectées en train de l'utiliser afin d'accéder sans autorisation à du matériel protégé par le droit d'auteur. En outre, lorsque vous utilisez le travail d'autrui, par exemple articles ou dissertations, n'oubliez pas de citer convenablement vos sources. A défaut, vous seriez passible de plagiat, ce qui pourrait vous causer beaucoup d'ennuis.

N'oubliez pas:

1. Vous êtes libre d'utiliser, de modifier et de distribuer des logiciels gratuits qui ne sont pas protégés par le droit d'auteur.
2. D'autres logiciels, en revanche, sont des logiciels partagés, qui sont donc gratuits pour une période d'essai spécifique.
3. Votre sphère privée pourrait être affectée et votre PC pourrait être endommagé par des virus ou d'autres «logiciels malveillants». Il vaut donc toujours mieux installer et actualiser en permanence des systèmes de protection tels qu'anti-virus, logiciels anti-dialer et pare-feu. Prenez toujours le soin de lire le guide relatif au programme que vous utilisez afin d'éviter de commettre les erreurs dont la liste figure ci-dessous.
4. Le matériel protégé par le droit d'auteur est généralement indiqué par un libellé standard, par exemple «tous droits réservés» ou d'autres formulations similaires; dans les cas où cela n'est pas évident, il est conseillé malgré tout de ne pas prendre de risques.
5. Les programmes Peer-to-Peer (P2P) que vous utilisez pour partager et télécharger des fichiers sont également

porteurs de certains risques. Il faut les comprendre de manière très approfondie pour pouvoir les utiliser sans aucun risque sur le plan de la sécurité:

a. Il se peut que vous ne téléchargiez pas toujours ce que vous vouliez: des contenus différents peuvent se cacher derrière le titre d'une chanson ou d'une vidéo. Dans le pire des cas, par exemple, ils peuvent contenir des photos d'enfants maltraités. Etudiez votre guide de programme particulier pour déterminer comment détecter les fichiers contrefaits, et n'utilisez que les sources dont vous savez qu'elles sont fiables; demandez à vos amis de vous dire quelles sont les sources à utiliser et celles à éviter.
b. Avant d'ouvrir un fichier téléchargé, prenez soin de le scanner pour détecter les virus; un autre risque assez fréquent tient à ce qu'un fichier téléchargé puisse contenir en fait des virus et des logiciels espions susceptibles de faire courir un risque aux PC, aux données personnelles et à la sphère privée.
c. Ne partagez pas l'intégralité de votre disque dur; vérifiez vos configurations afin de vous assurer que vous n'avez partagé que les fichiers que vous vouliez partager, et n'oubliez pas que partager des fichiers protégés par le droit d'auteur est un délit.

Commerce en ligne

Vous pouvez acheter des produits en ligne ou en utilisant un téléphone portable. Les achats peuvent être payés par carte de crédit ou, dans le cas des téléphones portables, en imputant le débit sur l'abonnement du téléphone portable. Il existe également des espaces en ligne consacrés à des échanges et à des achats de toutes sortes de produits, à des prix très compétitifs.

Une des différences fondamentales entre le commerce en ligne et le commerce traditionnel tient à ce qu'il est difficile d'identifier qui se trouve à l'autre bout de l'échange, et au risque de fraude qui rôde. Un des risques les plus répandus est celui du «phishing». C'est ce qui se produit lorsque l'on répond à des courriers électroniques factices, à du spam (pourriel), qui paraissent généralement venir d'une source réputée, par exemple une banque ou une société de carte de crédit. On vous demande alors de fournir beaucoup d'informations personnelles, par exemple détails de votre compte en banque, date de naissance, et ainsi de suite, qui seront ensuite utilisées dans un but criminel.

Une complication supplémentaire liée au commerce électronique a trait à la vente de produits ou de services réservés, sous une forme ou sous une autre, à des personnes ayant dépassé un certain âge. Par exemple, dans de nombreux pays il est illégal de vendre ou de fournir de l'alcool ou du tabac à des mineurs. De même, les jeux de hasard sont généralement limités à des personnes ayant dépassé un certain âge. Néanmoins, dans l'environnement en ligne, le vendeur peut avoir beaucoup de mal à déterminer l'âge de la personne qui se propose d'acheter le bien ou le service. Bon nombre de sociétés se contentent dès lors de demander à la personne de cocher une case pour confirmer qu'elle a bien l'âge minimum exigé.

Dans un certain nombre de pays, certaines entreprises commencent à utiliser des systèmes de vérification de l'âge liés à leurs procédures d'achat, mais cette technologie reste encore très nouvelle et limitée, bien qu'en plein essor. Acheter en ligne des produits réservés à des personnes

d'un certain âge, en mentant sur son âge pour pouvoir les acheter est susceptible de constituer un délit pénal pour l'acheteur tout comme pour le vendeur. Dans ce cas, vous pourriez perdre les biens et vous retrouver avec un casier judiciaire – donc, ne le faites pas.

En tout état de cause, il existe toute une série de tactiques qui peuvent vous aider à réduire les risques et à vous permettre de profiter des bonnes affaires offertes par le commerce en ligne:

1. Soyez très vigilant dans le choix des sites sur lesquels vous voulez faire des achats et assurez-vous de leur crédibilité. Rassemblez autant d'informations que possible sur le site en question, par exemple nom, adresse, numéro de téléphone et siège social de la société, descriptions des conditions contractuelles générales et en particulier modalités pour se retirer de l'achat; faites également des recherches sur la protection et la gestion des données personnelles et la sécurité des paiements; et comparez les prix, en recherchant le même article sur d'autres sites.
2. Les cartes de crédit prépayées ou rechargeables sont assorties de plafonds de dépenses qui peuvent contribuer à éviter les mauvaises surprises.
3. Avant d'acheter quoi que ce soit en ligne, assurez-vous que le site utilise un système sécurisé pour les transactions afin d'éviter par exemple le «flairage ou *sniffing*», qui est un moyen de capturer des données au cours de la transmission. Bien que bon nombre de sites incorporent des systèmes qui s'opposent à l'interception de données en transit, il se pourrait quand même que vos données soient volées si un pirate réussit à s'introduire dans le serveur de la société qui a enregistré les détails de votre carte de crédit. De toute évidence, en choisissant d'autres modes de paiement, vous pouvez éviter le risque de vous faire voler votre numéro de carte de crédit.
4. Si vous recevez un courrier électronique non sollicité vous offrant une affaire incroyable, il est plus que probable qu'il s'agisse d'une fraude.
5. Si quelque chose a l'air d'être trop beau pour être vrai, c'est très probablement le cas, et il vaut mieux l'oublier.
6. Dans le cas d'achats faits par le biais de téléphones portables et n'exigeant pas d'utiliser une carte de crédit, vérifiez quel est réellement le coût des services, les conditions auxquelles il est accordé et la manière de s'en retirer.

4. Conclusions

En respectant ces règles de base, vous pourrez échapper à la plupart des écueils que l'on peut rencontrer en ligne. S'il vous arrive de faire une expérience désagréable ou perturbante, parlez-en absolument à une personne de confiance. N'oubliez pas que vous avez le droit d'être protégé ainsi que la responsabilité d'agir de manière correcte, dans la vie réelle comme sur Internet.

Lectures recommandées et autres sources d'inspiration

Convention des Nations Unies sur les droits de l'enfant
www.unicef.org/crc/

Document de résultat du SMSI
www.itu.int/wsis

Activités de l'UIT en matière de cybersécurité
www.itu.int/cybersecurity

Initiative Protection de l'enfance en ligne (COP)
www.itu.int/cop

I*magine Your Future* – prévisions pour l'avenir
www.elon.edu/e-web/predictions/kid-zone/yourfuture.xhtml#kids%27%20predictions

The Internet Big Picture – statistiques relatives aux internautes et à la population
www.internetworldstats.com/stats.htm

Version adaptée aux enfants de «A World Fit for Children»
www.unicef.org/specialsession/wffc/child_friendly.html

Sondages d'opinion: ce que pensent les jeunes
www.unicef.org/polls

Connect Safely est destiné aux parents, aux adolescents, aux éducateurs, aux responsables de plaidoyer – à toutes les personnes qui s'intéressent au web social et s'y impliquent
www.connectsafely.org/

Déclaration de clôture des enfants et des adolescents lors du 3e Congrès mondial contre l'exploitation sexuelle
www.ecpat/net/WorldCongressIII/PDF/Outcome/WCHI_Outcome_Document_Final.pdf

Charte des enfants et des jeunes sur Internet dans le monde
www.iyac.net/children/index.htm

Un certain nombre de ressources de *Childnet* pour les jeunes
www.childnet-int.org/young-people/

Informations sur la sécurité sur Internet (accès aux sites en différentes langues)
www.safeinternet.org/ww/en/pub/insafe/index.htm
www.getnetwise.org/

Annexe 1

Contrat pour les parents

Je sais qu'Internet peut être un lieu formidable pour mes enfants. Je sais également que je dois jouer mon rôle pour les aider à assurer la sécurité de ces visites. Comprenant que mes enfants peuvent m'aider à cet égard, j'accepte de suivre les règles suivantes:

1. Je m'informerai sur les services et les sites web utilisés par mes enfants.
2. Je fixerai des règles et directives raisonnables pour l'utilisation de l'ordinateur par mes enfants, je discuterai de ces règles et je les afficherai près de l'ordinateur à titre de rappel.
3. Je ne réagirai pas de manière excessive si mes enfants me racontent quelque chose de «mal» qu'ils trouvent ou font sur Internet.
4. J'essaierai de faire connaissance avec les «amis en ligne» de mes enfants et leurs contacts figurant sur leurs listes de copains, tout comme j'essaye de faire la connaissance de leurs autres amis.
5. J'essayerai d'apporter à mes jeunes enfants un soutien et une surveillance étroits pour l'utilisation d'Internet, par exemple en essayant de garder leur ordinateur dans une zone familiale.
6. Je signalerai les activités et sites suspects et illégaux aux autorités compétentes.
7. J'établirai ou je me procurerai une liste de sites recommandés pour les enfants.
8. Je vérifierai fréquemment les sites que mes enfants ont consultés sur Internet.
9. Je chercherai des options pour filtrer et bloquer du matériel Internet inapproprié envers mes enfants.
10. Je parlerai à mes enfants de leurs explorations en ligne et j'entreprendrai des aventures en ligne avec eux aussi souvent que possible.

Je marque mon accord avec ce qui précède.

Signature des parents

_____

Date

_____

Je comprends que mes parents ont décidé d'appliquer ces règles et j'accepte d'aider mes parents à explorer Internet avec moi.

Signature de l'enfant

_____

Date

_____

Contrat pour l'enfant

Je sais qu'Internet peut être un lieu formidable à explorer. Je sais également qu'il est important pour moi de suivre des règles qui assureront ma sécurité lors de mes visites. J'accepte les règles suivantes:

1. Dans toute la mesure du possible, je choisirai un nom d'écran sûr et sensé pour moi-même, qui ne divulguera aucune information personnelle sur moi ou ma famille.
2. Je garderai tous mes mots de passe secrets.
3. Je discuterai avec mes parents de tous les différents programmes et applications que j'utilise sur mon ordinateur et sur Internet, et je discuterai avec eux des sites que je fréquente. Avant de télécharger ou de charger un nouveau programme ou d'adhérer à un nouveau site, je vérifierai d'abord avec mes parents pour m'assurer qu'ils sont d'accord.
4. Si j'envisage d'adhérer à un nouveau service en ligne, j'éviterai ceux qui réclament trop d'informations personnelles et j'essaierai d'opter pour ceux qui en demandent moins.
5. Je prendrai toujours des mesures pour déterminer quelles informations personnelles me concernant seront publiées par le service par défaut dans mon profil, et j'opterai toujours pour le degré de confidentialité maximum.
6. En aucune manière je ne partagerai mes informations personnelles ou celles de mes parents ou de n'importe quel autre membre de la famille en ligne ou avec une personne rencontrée en ligne. Cela inclut notamment, mais pas uniquement, le nom, l'adresse, le numéro de téléphone, l'âge ou le nom de l'école.
7. Je traiterai les autres comme je veux être traité moi-même.
8. Je ferai preuve de bonnes manières quand je suis en ligne, y compris en m'exprimant de façon correcte et respectueuse. Je ne participerai pas à des bagarres et n'utiliserai pas de menaces ni de gros mots.
9. Je ferai de ma propre sécurité personnelle ma priorité, car je sais qu'il existe sur Internet des gens qui se font passer pour ce qu'ils ne sont pas.
10. Je dirai honnêtement à mes parents quelles sont les personnes que je rencontre en ligne et je leur en parlerai sans qu'ils n'aient à me le demander. Je ne répondrai pas à des courriers électroniques ni à des messages instantanés émanant de personnes que mes parents n'ont pas approuvées.
11. Si je vois ou lis quelque chose de mauvais, de sale ou de malveillant, je me déconnecterai et j'en parlerai à mes parents afin qu'ils puissent veiller à ce que cela ne se reproduise pas.
12. Je dirai à mes parents si je reçois des images, des liens menant à des sites mauvais, des courriers électroniques ou des messages instantanés comportant des termes inappropriés ou si je suis dans un *chat room* avec des gens qui utilisent des jurons ou des gros

mots ou des termes méchants et haineux.

13. Je n'enverrai aucun courrier postal à une personne rencontrée en ligne sans l'accord de mes parents. Si je reçois au courrier un envoi venant d'une personne rencontrée en ligne, j'en parlerai immédiatement à mes parents (parce que cela signifie que cette personne possède des informations privées me concernant).
14. Je n'accepterai pas de faire en ligne une chose que l'on me demande si elle me met mal à l'aise, surtout si je sais que c'est le genre de choses que mes parents ne verraient pas d'un bon œil ou qu'ils n'approuveraient pas.
15. Je ne téléphonerai pas, n'écrirai pas de lettre et ne rencontrerai pas physiquement une personne rencontrée en ligne sans l'accord de mes parents ou sans qu'un adulte de confiance ne m'accompagne.
16. Je comprends que mes parents surveillent le temps que je passe en ligne et peuvent utiliser des logiciels pour contrôler ou limiter les sites que je fréquente en ligne. Ils le font parce qu'ils m'aiment et qu'ils veulent me protéger.

J'enseignerai à mes parents davantage de choses sur Internet afin que nous puissions nous amuser ensemble et apprendre de nouvelles choses cool.

Je suis d'accord avec ce qui précède.

Signature de l'enfant

_____

Date

_____

Je promets de protéger la sécurité de mon enfant en ligne en m'assurant que ces règles soient observées. Si mon enfant rencontre des situations peu sûres et m'en parle, je traiterai chaque situation avec maturité et bon sens, sans accuser quiconque, et au travers de cette situation, je m'emploierai calmement, avec le concours de mon enfant, à lui assurer des expériences Internet plus sûres à l'avenir.

Parent signature(s)

_____

Date

_____

Crédit photos: www.shutterstock.com, Violaine Martin/UIT, Ahone Ayeh Njume-Ebong/UIT

Union internationale des télécommunications
Place des Nations
CH-1211 Genève 20
Suisse
www.itu.int/cop

Imprimé en Suisse
Genève, 2010

Avec le soutien de:

Save the Children

Telefónica

CHIS

ins@fe