Lignes directrices pour les parents, les tuteurs et les éducateurs pour la protection de l'enfance en ligne

www.itu.int/cop

REMERCIEMENTS

Ces lignes directrices ont été préparées par l'UIT et une équipe d'auteurs contributeurs issus d'institutions actives dans le secteur des Technologies de l'Information et de la Communication (TIC), et n'auraient pas existé sans le temps, l'enthousiasme et le dévouement qu'ils y ont consacré.

L'UIT est reconnaissante aux auteurs suivants pour leur contribution, leur précieux temps et perspicacité (liste par ordre alphabétique):

- Cristina Bueti et Sandra Pandi (UIT)
- John Carr (*Children's Charities' Coalition on Internet Safety*)
- Ethel Quayle (Université d'Edimbourg, Royaume Uni)
- Janice Richardson (*Insafe Network*)
- Isabella Santa (*European Network and Information Security Agency*)
- Margareta Traung (*European Commission Safer Internet Programme*)
- Nevine Tewfik (Mouvement international des femmes pour la paix – Suzanne Mubarak: *Cyberpeace Initiative*)

Les auteurs souhaitent remercier John Carr du CHIS, Sonia Billard et Christiane Agbton-Johnson de l'UNIDIR, et Katerina Christaki de l'ENISA pour leurs lectures et commentaires détaillés.

L'UIT souhaite reconnaître la valeur de l'implication de Salma Abbasi du eWWG dans le cadre de l'initiative sur la Protection de l'enfance en Ligne (COP).

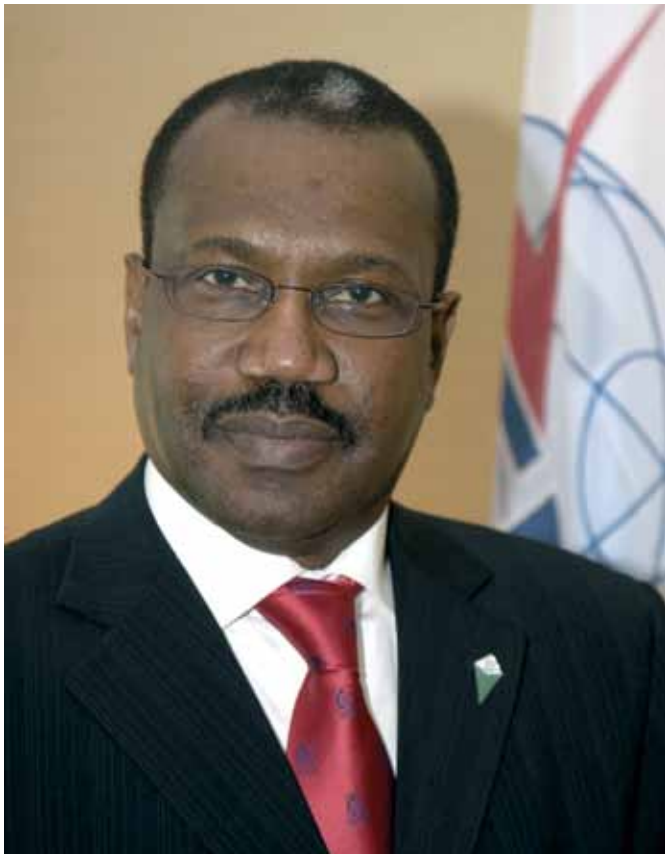
En relation avec ces premières lignes directrices, il est possible de trouver des informations et documents supplémentaires mis à jour de manière régulière en allant sur: www.itu.int/cop/

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

Table des matières


“La protection de l’enfance en ligne est un problème mondial, il faut donc trouver une réponse mondiale.”

Avant-propos



Je me réjouis de cette opportunité qui se présente à moi de partager avec vous ces premières lignes directrices développées avec l'aide inestimable de nombreuses parties prenantes.

La protection de l'enfance en ligne – dans cette ère d'accès massif large bande haut débit à Internet – est un problème crucial qui requiert une réponse mondiale coordonnée. Certes des initiatives locales, voire nationales, ont leur intérêt, cependant Internet ne connaît pas de frontières et une coopération internationale sera la clé de notre victoire dans les batailles qui s'annoncent.

Les parents, tuteurs et éducateurs sont des éléments indispensables dans la lutte contre le cybercrime et les cybermenaces, et je vous suis personnellement très reconnaissant de votre aide.

Hamadoun I. Touré

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

Résumé synoptique

Internet est source de bénéfices incommensurables pour les enfants du monde entier, le nombre de foyers connectés augmentant chaque année. Début 2009, il y avait 1,5 milliard de personnes en ligne, alors que début 1998 il y en avait moins de 200 millions.

Cependant, bien que personne ne conteste son potentiel bénéfique, Internet a également fait émerger de nouvelles et inquiétantes questions, notamment lorsque des enfants sont concernés.

Les jeunes d'aujourd'hui ont beaucoup de bon sens technique. Ils sont capables de maîtriser rapidement et facilement des programmes et des applications complexes que ce soit sur des ordinateurs, des terminaux mobiles ou d'autres équipements personnels et il semble qu'ils soient capables de le faire de façon quasi intuitive. D'autre part, lorsqu'il s'agit d'ordinateurs, de terminaux mobiles ou d'autres équipements personnels, les adultes ont en général besoin d'un manuel d'utilisation pour accomplir ce que les enfants considèrent comme des tâches assez faciles. Toutefois, les adultes apportent au débat concernant la sécurité électronique des précieuses compétences et expériences de la vie.

Il est crucial de déterminer ce que les enfants et les jeunes font en réalité en ligne par opposition à ce que les adultes pensent qu'ils font. Des recherches ont montré que de plus en plus d'enfants se connectent à Internet à l'aide de consoles de jeux et de terminaux mobiles, alors que de nombreux adultes n'ont même pas conscience qu'une connectivité est possible grâce à ces équipements.

Un problème essentiel est que les enfants et les jeunes ont tendance à accéder à Internet dans des lieux dans lesquels les adultes leur indiquent qu'ils sont en sécurité, à la maison ou à l'école par exemple. De nombreux parents et tuteurs adhèrent au malentendu commun selon lequel leurs enfants sont plus en sécurité à la maison lorsqu'ils utilisent un ordinateur que lorsqu'ils accèdent à Internet depuis l'extérieur de la maison. C'est un malentendu dangereux, et dans l'opération les enfants peuvent être exposés à des risques potentiellement dangereux, de la même manière que dans le monde réel.

Ces lignes directrices ont été développées par l'initiative sur la Protection de l'enfance en Ligne (COP)[1] dans le cadre du Programme mondial cybersécurité de l'UIT[2], avec pour objectif de poser les bases d'un cybermonde sûr non seulement pour les jeunes d'aujourd'hui, mais également pour les générations à venir.

Ces lignes directrices sont destinées à servir de schéma directeur pouvant être adapté et utilisé en

[1] www.itu.int/cop

[2] www.itu.int/osg/csd/cybersecurity/gca/

La convention des Nations Unies relative aux droits de l'enfant définit un enfant comme étant une personne de moins de 18 ans. Ces lignes directrices se concentrent sur les problèmes que rencontrent toutes les personnes de moins de 18 ans dans les différentes régions du monde. Toutefois, il est très improbable qu'un jeune utilisateur d'Internet de sept ans ait les mêmes besoins et intérêts qu'un enfant de 12 ans commençant le collège ou qu'un jeune de 17 ans proche de l'âge adulte. En différents endroits des lignes directrices nous avons adapté les avis ou recommandations pour les accorder aux différents contextes. Bien que l'usage de catégories assez larges puisse permettre d'élaborer un guide utile, il ne faut pas oublier qu'au final chaque enfant est différent. Il faut accorder une attention individuelle aux besoins spécifiques de chaque enfant. De plus, il existe de nombreux facteurs locaux, légaux et culturels qui auront un impact important sur la façon dont ces lignes directrices pourront être utilisées ou interprétées dans un pays ou une région donnés.

Il existe maintenant un ensemble substantiel de lois internationales et d'instruments internationaux qui sous-tendent et, dans de nombreux cas, imposent des actions destinées à protéger les enfants à la fois généralement et également plus spécifiquement dans le cadre d'Internet. Ces lois et instruments forment la base de ces lignes directrices. Ils sont résumés globalement dans la Déclaration et appel à l'action de Rio de Janeiro pour prévenir et éliminer l'exploitation sexuelle des enfants et des adolescents adoptée lors du troisième congrès mondial contre l'exploitation sexuelle des enfants et des adolescents, en novembre 2008.

adéquation avec les coutumes et lois locales. De plus, il serait appréciable que ces lignes directrices abordent des sujets pouvant affecter tous les enfants et jeunes de moins de 18 ans, chaque groupe d'âge ayant néanmoins des besoins différents. En effet, chaque enfant est unique et mérite une attention particulière.

Ces lignes directrices ont été préparées par l'UIT de manière tout à fait collaborative avec une équipe d'auteurs contributeurs issus d'institutions actives dans le secteur des technologies de l'information et de la communication (TIC), parmi lesquelles l'*EU Safer Internet Programme,* l'Agence européenne chargée de la sécurité des réseaux et de l'information (*European Network and Information Security Agency,* ENISA)[3], la *Children's Charities' Coalition on Internet Safety*, la *Cyberpeace Initiative* et l'Université d'Edimbourg (United Kingdom). Des contributions inestimables ont également été reçues de la part de gouvernements nationaux individuels et d'entreprises de hautes technologies partageant l'objectif commun de faire d'Internet un endroit meilleur et plus sûr pour les enfants et les jeunes.

L'UIT ainsi que les autres auteurs de ce rapport appellent toutes les parties prenantes à promouvoir l'adoption de politiques et de stratégies qui protègeront les enfants dans le cyberespace et à promouvoir un accès sûr aux ressources en ligne.

Cela conduira non seulement à la construction d'une société de l'information plus inclusive, mais cela permettra également aux pays membres de l'UIT de répondre à leurs obligations en matière de protection et prise en compte des droits de l'enfant comme l'indique la convention des Nations Unies relative aux droits de l'enfant[4], adoptée par la résolution 44/25 de l'assemblée générale des Nations Unies du 20 Novembre 1989, et le document du WSIS[5].

[3] www.enisa.europa.eu

[4] www.unicef.org/crc

[5] www.itu.int/wsis/outcome/booklet.pdf

Lignes directrices pour les parents, les tuteurs et les éducateurs

Cette section a pour objectif de fournir des lignes directrices aux parents, tuteurs et éducateurs afin de leur permettre d'aider les enfants à avoir une expérience d'Internet sûre et positive. Une liste plus détaillée de points à considérer se trouve page 49.

Parents, tuteurs et éducateurs		
	#	**Domaines essentiels à considérer**
1. Sûreté et sécurité de votre ordinateur personnel	a.	Maintenez l'ordinateur dans une pièce commune
	b.	Installez des logiciels antivirus et pare-feu
2. Règles	a.	Etablissez des règles domestiques concernant l'usage d'Internet et des terminaux personnels, en accordant une attention particulière à la vie privée, aux espaces inappropriés par rapport à l'âge, au danger de harcèlement et liés aux inconnus
	b.	Etablissez des règles concernant l'usage des terminaux mobiles

3. Education des parents, tuteurs et enseignants	a.	Les parents, tuteurs et enseignants doivent se familiariser avec les sites Internet utilisés par leurs enfants et avoir une bonne compréhension de la manière dont les enfants passent leur temps en ligne
	b.	Les parents, tuteurs et éducateurs doivent comprendre comment les enfants utilisent d'autres terminaux mobiles tels que les téléphones mobiles, les consoles de jeux, les lecteurs MP3, les PDA, etc.
4. Education des enfants	a.	Sensibilisez vos enfants aux risques associés au partage d'informations personnelles; à l'arrangement de rencontres réelles avec une personne rencontrées en ligne; à la mise en ligne de photographies; à l'usage de la webcam; etc.
5. Communication	a.	Communiquez avec vos enfants sur leurs expériences

1. Contexte

Le Sommet mondial sur la société de l'information (*World Summit on the Information Society,* WSIS), qui s'est tenu en deux phases à Genève (10-12 décembre 2003) et à Tunis (16-18 novembre 2005), s'est conclu sur l'engagement général de «construire une société de l'information centrée sur les personnes, inclusive et orientée vers le développement, dans laquelle tout le monde peut créer, accéder, utiliser et partager les informations et le savoir» (Déclaration de principe de Genève, paragraphe 1).

Lors du WSIS, les dirigeants de la communauté internationale ont confié à l'UIT le point d'action C5: «créer confiance et sécurité lors de l'usage des TIC».

Les résultats du WSIS ont également spécifiquement reconnu les besoins des enfants et des jeunes en matière de protection dans le cyberespace.

L'Engagement de Tunis a reconnu «le rôle des technologies de l'information et de la communication (TIC) dans la protection des enfants et dans l'amélioration du développement des enfants» ainsi que le besoin de «renforcer les actions destinées à protéger les enfants des abus et à défendre leurs droits dans le contexte des TIC».

Il est en général admis[6], que nous savons où se trouvent nos enfants tous les jours, avec qui ils sont, et ce qu'ils font. Cependant dans le monde numérique, où même nos plus jeunes enfants passent de plus en plus de temps, nous en sommes souvent réduits au rôle de spectateur et nombre d'entre nous subissons un «coup de bambou numérique».

[6] www.parenting.com/article/Mom/Relationships/How-to-Spy-on-Your-Child-Online

“Les adultes apportent au débat concernant la sécurité électronique leurs compétences et expériences de la vie ”

Les enfants, même les plus jeunes, peuvent tout à fait mieux comprendre les technologies actuelles que des éducateurs ou parents.

Les enfants d'aujourd'hui n'ont que l'expérience d'un monde rempli d'éléments numériques où la technologie s'entremêle dans tous les aspects de leur vie.

Elle informe de leurs amitiés, de leur éducation et de leur compréhension du monde et des personnes qui les entourent. Pendant ce temps nous, en tant qu'adultes, tentons de trouver quelles règles définir et comment les appliquer.

Le problème est que ce sujet n'est pas abordé dans les livres d'éducation destinés aux parents; ce chapitre n'a pas encore été écrit et la société n'a pas encore eu le temps de définir des normes.

Nous avons un âge légal pour boire et un âge légal pour conduire, mais il n'y a pas de certitude conventionnelle solide concernant l'âge auquel les enfants peuvent aller seuls en ligne en toute sécurité, ou envoyer des textes à leurs amis via leur téléphones mobiles, ou concernant le rôle des parents dans la surveillance de nos vulnérables et souvent naïfs enfants lors de leurs activités en ligne.

Il existe une différence déconcertante entre ce que les parents pensent que leurs enfants savent et ce que les enfants savent en réalité.

Alors que 92% des parents affirment avoir établi des règles concernant les activités en ligne de leurs enfants, 34% des enfants indiquent que leurs parents ne l'ont pas fait. Ces chiffres sont cohérents quelque soit le pays dans le monde:

En France, 72% des enfants surfent en ligne seuls, et bien que 85% des parents connaissent l'existence des logiciels de contrôle parental, seuls 30% en ont installé un.

En Corée, 90% des maisons ont une connexion haut débit peu chère, et jusqu'à 30% des Coréens de moins de 18 ans ont un risque d'addiction à Internet, passant sur Internet deux heures ou plus par jour.

Au Royaume-Uni, 57% des enfants de 9 à 19 ans indiquent avoir vu de la pornographie en ligne, 46% avouent avoir donné sur Internet des informations qu'ils n'auraient pas dû et 33% admettent avoir été intimidés en ligne.

En Chine, 44% des enfants indiquent avoir été approchés par des inconnus en ligne, et 41% ont parlé à des inconnus de sexe ou de sujets qu'ils ont trouvé gênants.

Afin de répondre à ces défis en croissance, l'UIT, avec l'aide d'autres parties prenantes, a lancé l'initiative sur la Protection de l'enfance en Ligne (*Child Online Protection,* COP)[7].

La COP a été développée par l'UITdans le cadre du Programme mondial cybersecurité (*Global Cybersecurity Agenda*)[8] et a été établi en tant que réseau collaboratif international d'action destiné à promouvoir la protection en ligne des enfants et des jeunes au niveau

[7] www.itu.int/cop

[8] www.itu.int/osg/csd/gca

mondial, en fournissant un guide quant à un comportement en ligne sûr en coopération avec d'autres agences des Nations Unies et partenaires.

Les objectifs essentiels de la COP sont:

- d'identifier les risques et vulnérabilités élémentaires des enfants et des jeunes dans le cyberespace;
- de créer une conscience des risques et problèmes à travers divers médias;
- de développer des outils pratiques afin d'aider les gouvernements, organisations et éducateurs à minimiser ces risques;
- de partager les connaissances et expériences en facilitant les partenariats stratégiques internationaux pour définir et mettre en œuvre des initiatives concrètes;
- Ces lignes directrices ont été préparées dans le cadre de la COP et ont pour objectif de fournir des informations, des avis et des astuces en matière de sécurité aux parents, tuteurs et éducateurs concernant la protection de l'enfance en ligne.

2. Les enfants et les jeunes en ligne

Internet a continué d'évoluer de façon spectaculaire au cours des dernières années. De nouveaux services, tels que les blogs, Wikipedia, MySpace, YouTube, et les jeux en ligne ont augmenté la connectivité d'Internet, encourageant le réseautage social et permettant aux personnes surfant sur Internet de créer leur propre contenu. Le nombre de blogs continue de doubler tous les cinq mois au cours des deux dernières années; l'utilisation de sites de réseautage social tels que Bebo, Facebook, Habbo et Twitter se multiplie d'année en année; et depuis les trois dernières années, la communication entre utilisateurs du web est devenue la source de trafic la plus importante sur Internet.

Les enfants et les jeunes sont des utilisateurs actifs et enthousiastes des TIC pour ce qui est des discussions virtuelles et du partage d'informations personnelles. Cela offre une variété d'opportunités positives de participation, de créativité et d'éducation. Cela permet également une communication entre jeunes au-delà des frontières nationales, religieuses et culturelles. Par exemple, le tableau ci-dessous décrit le type d'expériences en ligne que les enfants sont le plus susceptibles d'avoir lorsqu'ils accèdent aux mondes virtuels[9]:

[9] ENISA, *Children on virtual worlds – What parents should know*, septembre 2008, Les enfants dans les mondes virtuels – ce que les parents doivent savoir, disponible en anglais sur www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf

Type d'acteur	Intéressé par	Susceptible d'être	Caractéristiques
Explorateurs-investigateurs	Mener une quête, résoudre un mystère, partir en voyage, être «à l'extérieur»	Les enfants les plus confiants, sans distinction d'âge ou de sexe	Ils examinent les détails, sont curieux et communicatifs, ont un engagement imaginatif avec le mystère
Self-stampers	Se présenter au monde	Les enfants des deux sexes, probablement plus âgés	Garçons et filles souhaitent «apporter leur marque» sur leur avatars, parfois avec leur propre visage; les filles plus âgées habillent et maquillent leur avatars. Garçons et filles souhaitent s'exprimer à travers la création d'une maison ou d'une «base».
Arriviste	Accéder à un statut social dans le jeu	Les enfants à la fois plus jeunes et plus âgés; faible biais sexuel (légèrement plus de garçons que de filles)	Esprit de compétition; se préoccupent de leur classement et l'affichent aux autres
Combattants	La mort et la destruction, la violence et les super pouvoirs	Garçons, faible biais envers les garçons plus âgés	Les enfants expriment de la frustration lorsqu'ils n'ont pas les moyens de s'exprimer; offrir des opportunités de «gagner» et de «battre des adversaires» diminue la frustration.

Type d'acteur	Intéressé par	Susceptible d'être	Caractéristiques
Collectionneurs-consommateurs	Accumuler tout ce qui a une valeur perçue dans le système	Garçons et filles plus âgés	Ils collectionnent les pages et les pièces, cherchent les boutiques, les opportunités de faire des cadeaux, une économie et une place où mettre leurs possessions
Utilisateurs avancés	Donner à tout le monde le bénéfice de leur savoir et de leur expérience	Expert dans les jeux, la géographie de l'environnement, les systèmes	Ils passent de nombreuses heures à jouer et à explorer les jeux, avec un profond intérêt pour le fonctionnement du jeu
Constructeurs d'écosystèmes	Créer de nouveaux territoires, de nouveaux éléments de l'environnement et peupler cet environnement	Les enfants les plus jeunes (imaginant des mondes sans aucune règle), ou des enfants plus âgés (imaginant des mondes avec des règles et systèmes – maisons, écoles, boutiques, transport, économie)	Enfants exprimant de la frustration lorsqu'ils n'ont pas les moyens de s'exprimer; les systèmes (ou leur absence) qui gouvernent l'environnement sont attrayants.
Protecteurs	S'occuper de leurs avatars et animaux domestiques	Garçons et filles les plus jeunes et filles plus âgées	Les enfants veulent jouer et rencontrer d'autres enfants pour apprendre à leur avatars des choses telles que nager et pour avoir un endroit où les faire dormir. Les animaux domestiques virtuels sont également attrayants.

Internet est un outil neutre de diffusion des données pouvant être utilisé à de bonnes ou mauvaises fins.

D'un côté, par exemple, son potentiel en tant que source d'éducation de personnes de tous âges et de toutes capacités est énorme.

De l'autre, Internet peut être utilisé pour créer des pièges en ligne et exploiter les utilisateurs à des fins criminelles, et malheureusement les enfants figurent parmi ceux qui sont le plus vulnérables à ces pièges.

Il est important de se rappeler qu'Internet n'est pas seulement un outil de communication pouvant éventuellement affecter de manière négative le bien-être des enfants.

Au cours des dernières années, l'utilisation de téléphones mobiles par les jeunes s'est accrue de manière spectaculaire et les enfants utilisent leurs téléphones mobiles pour accéder à Internet virtuellement, quelque soit l'endroit où ils se trouvent.

Cela augmente la probabilité d'être exposé aux dangers en ligne sans supervision d'un adulte.

En Corée par exemple, l'âge moyen auquel on offre aux enfants leur premier téléphone mobile est aux alentours de 8 ans.

Il est important de se rappeler que les téléphones mobiles eux-mêmes ont beaucoup évolué récemment.

Les équipements peuvent maintenant être utilisés pour envoyer des messages vidéo, pour les services de divertissement (téléchargement de jeux, musique et vidéos), ainsi que pour accéder à Internet et aux services liés à la localisation.

Les risques potentiels auxquels sont soumis les enfants accédant à Internet via leur téléphones mobiles ou autres équipements mobiles sont les mêmes que dans le cas d'un accès à Internet via une connexion filaire.

La grande différence entre l'accès à Internet via le téléphone mobile ou l'ordinateur portable d'un enfant et l'accès traditionnel à Internet via l'ordinateur de la maison est la nature très privée de ces terminaux mobiles personnels.

Lorsque des terminaux personnels sont utilisés principalement par des adolescents, les parents ne peuvent typiquement pas appliquer de supervision directe comme ils le feraient sur un ordinateur à la maison.

Les parents doivent parler à leurs enfants de l'usage qu'ils font et s'assurer qu'ils activent les contrôles sur les terminaux de leurs enfants lorsqu'ils achètent ou utilisent pour la première fois ces terminaux.

Un cas d'étude: les jeunes Egyptiens et Internet

Le Groupe de réflexion sur la sécurité de la jeunesse égyptienne sur Internet (*Egyptian Youth Internet Safety Focus Group*, Net-Aman) est composé de 11 membres âgés de 18 à 28 ans et fait partie intégrante de l'initiative plus générale *Cyber-Peace* développée par le Mouvement international des femmes pour la paix – Suzanne Mubarak avec l'aide d'un certain nombre de partenaires.

Le nom du groupe de réflexion est Net-Aman (Net-sécurité en arabe), il a été choisi par les jeunes membres.

Le mandat de ce groupe est d'augmenter la prise de conscience de la sécurité sur Internet et l'énorme potentiel des TIC avec l'objectif d'offrir aux enfants et aux jeunes une chance d'identifier eux-mêmes les contenus nuisibles et de décider de la meilleure façon de se comporter face à ses contenus à travers une approche participative.

La session de formation initiale de Net-Aman a produit un questionnaire que les membres ont utilisé pour saisir une vue instantanée des préoccupations et espoirs des enfants et des jeunes concernant l'utilisation d'Internet en Egypte.

Chaque jeune devait aller dans les écoles et universités et soumettre un rapport sur les conclusions de l'étude lors de la deuxième session de formation en mars 2008. L'étude a couvert un échantillon de jeunes représentant des groupes d'âges divers compris entre 8 et 22 ans.

Une telle étude a aidé Net-Aman à comprendre comment les jeunes en Egypte se sentent par rapport à Internet et par rapport à leur sécurité.

Environ 800 jeunes Egyptiens ont répondu à l'étude de jeune à jeune intitulée «Les jeunes Egyptiens et Internet».

Les enfants et les jeunes questionnés ont affirmé que:

- Ils ne sont surveillés par aucun adulte lorsqu'ils utilisent Internet.
- Concernant les risques et les défis d'Internet en Egypte, ils ont listé: les contenus inappropriés représentent le principal risque en ligne, puis les virus et les logiciels espions, les contenus violents, la copie pour les devoirs (plagiat), et en dernier les brimades en ligne.
- L'un des résultats les plus choquants de l'étude fut le fait que la plupart des jeunes partagent leurs informations personnelles, nom complet, âge, photographies, informations scolaires et numéros de téléphone sur Internet sans se préoccuper des conséquences.

À la lumière des résultats de cette étude et en ligne avec le Groupe de réflexion sur la sécurité de la jeunesse égyptienne sur Internet (Net-Aman), les jeunes membres vont continuer à contribuer et participer aux efforts qui aideront à faire émerger une conscience concernant les problèmes de protection de l'enfant en ligne pour les jeunes Egyptiens.

Pour plus d'informations, veuillez consulter le site web de *Cyberpeace Initiative*: www.smwipm.cyberpeace-initiative.org

3. Parents, tuteurs et éducateurs

Définition des parents, tuteurs et éducateurs

Plusieurs sites sur Internet font référence aux parents de manière générique (par exemple sur une «page destinée aux parents» et font référence au «contrôle parental»), il peut donc être utile de définir les personnes qui doivent idéalement s'assurer que les enfants utilisent les sites Internet en toute sécurité et de manière responsable et accorder leur consentement pour accéder à certaines sites web spécifiques.

Dans ce document, le terme «parents» fera référence à la mère et/ou au père naturels d'un enfant ou à la personne à laquelle la garde de l'enfant à été accordée.

Le monde actuel présente une multitude de cas dans lesquels des personnes autres que les parents naturels peuvent s'occuper d'enfants.

Elles sont souvent désignées sous les termes de tuteurs ou gardiens, et il est important et impératif de reconnaître le rôle qu'ils peuvent jouer lorsque les enfants dont ils ont la garde sont en ligne.

Un éducateur est une personne qui travaille systématiquement à améliorer la compréhension d'un sujet par une autre personne.

Le rôle des éducateurs englobe à la fois ceux qui donnent des cours dans des classes et ceux qui de manière plus informelle travaillent, par exemple, dans les sites de réseautage social à fournir des

informations concernant la sécurité en ligne ou qui dirigent des cours destinés à une communauté ou à une école pour permettre aux enfants de rester en sécurité en ligne.

Le travail des éducateurs va varier selon le contexte dans lequel ils travaillent et la tranche d'âge des enfants (ou adultes) qu'ils cherchent à éduquer.

Ce sont tous ceux qui sont en contact avec des enfants et des jeunes – parents, professeurs, assistants sociaux, bibliothécaires, travailleurs sociaux, responsables de jeunes et les membres de la famille élargie, y compris les grands-parents. Il est important de noter que les enfants sous la garde des services sociaux représentent un groupe particulièrement vulnérable et nécessitent en tant que tel une attention particulière.

Il est également important de considérer le rôle du parrainage par les pairs, car ces individus seront des éducateurs dans un certain sens.

Ce qu'ignorent de nombreux parents, tuteurs et éducateurs

Une analyse récente réalisée par l'ENISA a mis en évidence que dans la plupart des cas, les parents et tuteurs ne sont pas conscients des détails concernant les expériences en ligne auxquelles leurs enfants sont susceptibles de faire face et les vulnérabilités liées aux différentes activités en ligne.

Les enfants peuvent être en ligne à l'aide de différentes plate-formes et équipements, parmi lesquels:

1. les ordinateurs personnels
2. les téléphones mobiles
3. les assistants numériques personnels (*Personal digital assistant*, PDA)

Selon le type de plate-forme utilisée et les fonctionnalités disponibles, l'expérience de chacun sera différente. Par exemple:

Fonctionnalité	Description
Créer des profils	Saisir des informations les concernant
Interagir avec les autres	Partager des informations et idées avec d'autres utilisateurs par le biais de fonctionnalités de discussions virtuelles (chat), blogs , messagerie instantanée, forum de discussion et de Voix sur IP (*Voice over Internet Protocol*, VoIP)
Créer un avatar	Choisir une image graphique les représentant et établir leur identité sur le site Internet
Jouer à des jeux	Mettre leur esprit au défi et fournir des activités auxquelles participer en ligne
Répondre à des quizz	Des défis, tels que des exercices de réflexion, en général avec une récompense pour leur participation. Fournit également l'occasion d'une compétition entre amis ou groupes d'amis sous la forme de «classements»
Faire des dessins, animations, bandes dessinées et gadgets	Egalement appelé UGC (*user-generated content*) ou contenu généré par les utilisateurs, de nombreux enfants apprécient de créer leur propre contenu qu'ils partagent avec leur communauté et se développent de façon créative lorsqu'ils collaborent avec d'autres membres de leur communauté virtuelle
Créer du contenu, de la musique et de la danse à de la vidéo	L'auto-édition s'est ouverte à tous les âges et peut être un excellent exutoire créatif
Acheter des produits	Certains services peuvent permettre aux utilisateurs d'acheter des produits ou des services à l'aide d'argent réel
Mettre en ligne des photographies ou toute autre information	Certains services peuvent permettre aux enfants de télécharger des photographies et des informations. Certains filtrent les contenus personnels et/ou inappropriés
Télécharger de la musique	Certains services peuvent permettre aux enfants de télécharger de la musique
Voir des publicités concernant des produits/services	Les sites Internet sont souvent subventionnés par la publicité

Les jeunes vont en ligne pour un grand nombre de raisons différentes parmi lesquelles on peut citer les suivantes[10]:

1. Interagir avec des amis dans un nouvel environnement, partageant en temps réel des intérêts communs avec d'autres.
2. Créer et se joindre à des communautés ou des groupes d'intérêt commun, par exemple la musique, le football, etc. Communiquer des idées et des informations sur des domaines d'intérêt par le biais de blogs, de messageries instantanées et d'autres outils.
3. Rencontrer de nouvelles personnes et éventuellement se faire de nouveaux amis.
4. Créer et partager des contenus originaux et personnels, tels que des images, des photographies et des vidéos pour augmenter les opportunités de s'exprimer.
5. Créer, éditer et partager de la musique.
6. Jouer à des jeux.
7. Etablir leur propre espace, même lorsque les parents et tuteurs sont présents.
8. Faire des expérimentations avec leur identité, les nouveaux espaces et frontières sociaux.

Même si l'expérience utilisateur est différente lorsque l'accès à un site Internet a lieu via un téléphone mobile ou un PDA plutôt que via un ordinateur personnel, les risques et vulnérabilités liés à l'utilisation d'Internet sont les mêmes, quelque soit la plate-forme.

1. Un problème essentiel vient du fait que les enfants et les jeunes accèdent à Internet dans des endroits dont nous leur disons qu'ils sont sûrs, tels l'école ou la maison. Les parents et les tuteurs font la même erreur de compréhension en indiquant souvent qu'ils préfèrent que leurs enfants soient à la maison en train d'utiliser un ordinateur, plutôt qu'à l'extérieur sans savoir où ils sont. Internet peut évidemment emmener les enfants et les jeunes n'importe où et ils peuvent être exposés à des risques de la même manière que dans le monde réel (voir cas page 21).

[10] Home Office, *Home office task force on child protection on the internet – Good practice guidelines for the providers of social networking and other user interactive services 2008*, 2008, disponible ici: http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance?view=Binary (dernière visite le 16 juin 2008).

Cas d'étude: La vie privée en péril

De nombreux utilisateurs n'ont pas conscience de la quantité d'informations personnelles qu'ils donnent en ligne ou même comment cela se produit!

Parmi les méthodes, citons:

- l'oubli de cliquer sur les paramètres de confidentialité, et
- la fourniture de plus d'informations que nécessaires

Pour les enfants et les jeunes, cela les rend néanmoins vulnérables à un (éventuel) contact inapproprié d'un pair, d'un jeune plus âgé ou même d'un adulte. Les enfants peuvent également innocemment donner des informations les concernant en:

- complétant n'importe quel type de formulaire (pour un concours ou un enregistrement par exemple)
- envoyant des profils personnels
- créant un site web

Il est important que les parents n'exagèrent pas les risques ou ne fassent pas indûment peur aux enfants dans leur façon d'aborder les risques auxquels ils peuvent être exposés en ligne.

Savoir comment les enfants peuvent innocemment donner des informations en ligne et avec quelle facilité ces informations les concernant peuvent être découvertes par des étrangers, fait partie des choses importantes à prendre en considération.

Les enfants ont besoin d'apprendre qu'il existe de nombreuses bases de données capables de fournir des informations sur leur adresse, numéro de téléphone et adresse électronique.

Il faut encourager les enfants et les jeunes à utiliser les paramètres de confidentialité chaque fois qu'ils sont en ligne et à prévenir un adulte responsable lorsqu'on leur demande des informations (physiques) personnelles ou lorsqu'ils ne sont pas à l'aise avec leur communication en ligne.

Ci-dessous se trouve une fausse discussion d'un salon virtuel (*chatroom*) dont les forces de l'ordre pensent qu'il s'agit d'un exemple réaliste de discussion en ligne. Imaginons un pédophile prédateur assis et prenant des notes sur cet enfant, et utilisant ces informations pour les attirer plus tard. Votre enfant se ferait-il avoir? Malheureusement, c'est le cas pour certains enfants.

Enfant: Je déteste ma mère! Je sais que c'est de sa faute si mes parents divorcent.

Prédateur: Je sais. Mes parents divorcent aussi.

Enfant: Nous n'avons plus jamais assez d'argent non plus. Chaque fois que je veux quelque chose, elle dit la même chose: «On ne peut pas se le permettre». Quand mes parents étaient ensemble, je pouvais acheter des trucs. Maintenant, ce n'est plus possible.

Prédateur: Moi aussi. Je déteste ça!

Enfant: J'ai attendu six mois que le nouveau jeu sur PC sorte. Ma mère m'avait promis de me l'acheter à sa sortie. Elle avait promis! Maintenant il est sorti. Est-ce que je peux l'acheter? Non. «On n'a pas assez d'argent!». Je déteste ma mère!

Prédateur: Oh! Je suis tellement désolé! Je l'ai eu! J'ai un oncle vraiment cool qui m'achète des trucs tout le temps. Il est vraiment riche.

Enfant: Tu as troooop de chance. J'aurais aimé avoir un oncle riche et cool.

Prédateur: Hé! J'ai une idée! Je vais demander à mon oncle s'il veut bien t'en acheter un aussi... Je t'ai dit qu'il est vraiment cool. Je parie qu'il va dire oui.

Enfant: C'est vrai?! Merci!!

Prédateur: BRB (langage en ligne pour dire «je reviens de suite»)... Je vais l'appeler.

Prédateur: Devine quoi? Il est d'accord. Il va t'acheter le jeu!

Enfant: Wouah, vraiment? Merci. Je n'y crois pas!!!

Prédateur: Où habites-tu?

Enfant: J'habite en IdF. Et toi?

Prédateur: J'habite Paris. Mon oncle aussi. On n'est pas loin.

Enfant: Super!

Prédateur: Est-ce qu'il y a un centre commercial près de chez toi? On pourrait s'y retrouver.

Enfant: OK. J'habite près de la Croix Blanche.

Prédateur: Oui, je connais. Pas de prob. Que dis-tu de samedi?

Enfant: Cool.

Prédateur: On peut aller au MacDo aussi si tu veux. On s'y retrouve à midi.

Enfant: OK. Où?

Prédateur: Devant le magasin de jeux vidéos. Oh! Le nom de mon oncle est George. Il est vraiment cool.

Enfant: Super... merci, j'apprécie vraiment. Tu as tellement de chance d'avoir un oncle riche et cool.

Le samedi arrive, et l'enfant va au centre commercial et rencontre un adulte devant le magasin de jeux vidéos. Il se présente comme étant «Oncle George» et explique que son neveu est déjà au MacDo en train de les attendre.

L'enfant n'est pas à l'aise, mais l'oncle rentre dans le magasin et achète le jeu à 60 €. Il sort du magasin et le tend à l'enfant, qui est immédiatement neutralisé et ravi.

Les avertissements face aux dangers que représentent les inconnus ne s'appliquent pas. Il ne s'agit pas d'un inconnu – c'est «Oncle George», et si besoin était, le jeu vidéo en est la preuve. L'enfant monte sans hésiter dans la voiture d'Oncle George pou rejoindre son ami au MacDo. Le reste de l'histoire fait l'objet d'un reportage aux informations du soir.

C'est dégoûtant. Cela nous prend aux tripes, mais cela arrive. Certes peu souvent, mais suffisamment pour que l'on fasse de la prévention. (Plusieurs centaines de cyberprédateurs sont arrêtés chaque année.) Que cela arrive une seule fois est déjà de trop lorsqu'il s'agit de votre enfant. Savoir comment ils opèrent et leurs astuces vous aidera à enseigner à votre enfant ce qu'il faut faire pour éviter de devenir une victime.

Source: www.wiredkids.org/parents/parry_guide.html

Les risques et vulnérabilités en ligne liés à l'utilisation d'Internet

L'exposition à des contenus illégaux et malfaisants, tels que la pornographie, les paris et d'autres contenus inappropriés pour des enfants et les contacts avec d'autres utilisateurs. Dans la plupart des cas, les opérateurs de ces sites ne prennent pas de mesures effectives pour restreindre l'accès des enfants à leurs sites.

La création, la réception et la diffusion de contenus illégaux et malfaisants.

Prétendre être quelqu'un d'autre, souvent un autre enfant, dans le cadre d'une tentative délibérée de nuire, de harceler ou d'intimider quelqu'un d'autre.

Les contacts indésirables, en particulier de la part d'imposteurs adultes se faisant passer pour des enfants.

La divulgation d'informations personnelles engendrant la possibilité de dommages physiques.

Les tentatives criminelles de se faire passer pour des utilisateurs d'Internet, en premier lieu dans l'espoir d'obtenir un gain financier. Dans certains cas, cela inclut le vol d'identité, bien que ce soit en général associé à des tentatives d'escroquer des adultes.

Les dommages physiques via des rencontres dans la vie réelle de connaissances faites en ligne, avec possibilité d'abus physique et sexuel.

La prise pour cible via du multipostage abusif (spam) et des publicités d'entreprises utilisant des sites Internet pour promouvoir des produits ciblés par âge et/ou intérêt.

L'usage excessif au détriment d'activités sociales et/ou d'extérieur importantes pour la santé, le renforcement de la confiance, le développement social et le bien-être en général.

Les brimades et le harcèlement.

Les comportements d'automutilation, destructifs et violents tels que le «*happy slapping*» ou vidéolynchage.

Utilisation compulsive ou excessive d'Internet ou des jeux en ligne

L'exposition au racisme ou autres discours et images discriminatoires.

La diffamation ou l'atteinte à la réputation.

La violation de ses propres droits ou de ceux des autres au travers du plagiat et du téléchargement de contenus (en particulier de photographies) sans autorisation. Il a été démontré que prendre et télécharger des photographies sans autorisation est dommageable pour les autres.

La violation des droits d'auteur d'autrui, par exemple en téléchargeant de la musique, des films ou des programmes télévisuels pour lesquels il faudrait payer.

Se baser sur ou utiliser des informations inexactes ou incomplètes, ou des informations provenant d'une source inconnue ou douteuse.

L'utilisation non autorisée de cartes bancaires: les cartes bancaires des parents ou d'autres personnes pouvant être utilisées pour payer les frais d'adhésion, ou d'autres frais liés à des services ou des marchandises.

La présentation déformée de l'âge de quelqu'un: soit un enfant prétendant être plus âgé afin d'avoir accès à des sites inappropriés, soit quelqu'un de plus âgé pour les mêmes raisons.

L'utilisation du compte de messagerie des parents sans leur accord: lorsque l'accord des parents est nécessaire pour activer le compte d'un enfant sur des sites de mondes virtuels, les enfants peuvent usurper l'identité de leurs parents pour accéder à leur comptes de messagerie. Une fois activés certains comptes peuvent être difficiles à supprimer pour les parents.

La publicité indésirable: certaines entreprises font du publipostage abusif (spam) à destination des enfants par le biais de sites de mondes virtuels pour vendre des produits. Cela soulève le problème du consentement de l'utilisateur et comment il doit être obtenu. La législation en la matière est insuffisante et il est clairement très difficile de déterminer à quel moment les enfants sont capables de comprendre les échanges de données. En effet, comment appliquer ces règles sur Internet est déjà un problème majeur et l'accès par téléphones mobiles l'accentue encore.

Plus spécifiquement, ce qui suit présente les plus grandes préoccupations des éducateurs, car ils se

sentent souvent mal équipés pour y faire face.

Le réseautage social – la manière dont les enfants et les jeunes vivent leur vie à l'aide des espaces sociaux est très différente de tout ce à quoi sont habitués les éducateurs. Nombre d'entre eux ne comprennent pas pourquoi il est si important d'avoir autant d'«amis» dans une liste de contacts, mais le nombre d'amis est considéré comme l'équivalent de la popularité des jeunes utilisateurs.

Le sexting (mot valise de sexe et texting) – le phénomène relativement nouveau selon lequel les enfants et les jeunes prennent eux-mêmes des risques et qui consiste en l'envoi par des enfants et des jeunes, sur Internet ou à des amis à l'aide de technologies mobiles, d'images provocantes sexuellement les mettant eux-mêmes en scène.

La façon dont les enfants utilisent les nouveaux médias – par opposition à la façon dont nous pensons qu'ils les utilisent. Il existe de bonnes recherches disponibles (dans chaque pays) qui peuvent permettre de servir de base à ce travail (voir également le site *EU Kids Online* pour les résumés des problèmes, risques, etc. dans l'UE: www.eukidsonline.net).

Où chercher de l'aide? De nombreux pays ont des lignes téléphoniques auxquelles les enfants et les jeunes peuvent faire part d'un problème. Une large publicité leur est faite et différents pays ont des approches différentes pour faire passer le message. Il est important que les enfants et les jeunes réalisent qu'il n'est jamais trop tard pour rapporter un problème et qu'en le faisant ils peuvent aider d'autres enfants.

Comment les éducateurs peuvent risquer de se retrouver victimes d'intimidations (par exemple, par des enfants et des jeunes qui créent des sites haineux concernant des enseignants ou d'autres professionnels). Les éducateurs ont besoin de sentir qu'ils peuvent avoir confiance et utiliser la technologie de manière sûre. De nombreux éducateurs se sentent mal équipés pour faire face à certains de ces problèmes et ne savent pas comment effectivement faire retirer des choses des sites, etc. Le site web teachtoday fournit une aide excellente concernant ce sujet et d'autres sujets en relation (www.teachtoday.eu).

Il est important de souligner (comme indiqué ci-dessus) que bien que certains éducateurs ne maîtrisent pas techniquement les technologies autant que les enfants et les jeunes, ils ont des compétences et une expérience de la vie qui leur permettent de guider et de proposer des avis et un soutien. Il faut le répéter aux éducateurs lors des formations sur les problèmes de sécurité en ligne.

L'étude OPTEM[11] suggère toutefois que les risques identifiés par les enfants eux-mêmes semblent être plus en relation avec Internet qu'avec les téléphones mobiles, ils comprennent:

Les risques liés à l'ordinateur (tels que les virus ou le piratage informatique).

L'apparition non sollicitée d'images, ou l'accès par erreur à des sites web indésirables affichant de la violence ou de la pornographie (les enfants plus âgés ont tendance à dédramatiser l'impact d'une exposition accidentelle).

Les inconvénients et les fraudes.

Les attaques à caractère sexuel par des adultes malveillants.

Alors que les enfants reconnaissent qu'ils se permettent parfois eux-mêmes des comportements risqués, ils ne montrent pas une grande inquiétude quant aux risques inhérents à ce type de comportements et affichent une préférence pour une tentative de résolution du problème par eux-mêmes ou au sein du groupe de pairs. Cela suggère qu'ils ne font appel à leurs parents ou à d'autres adultes qu'en cas de problèmes potentiellement «dramatiques». Il s'agit d'un problème particulièrement avec les garçons plus âgés qui ont plus tendance à utiliser le bouton danger[12] (tel que développé par le Groupe de travail *Virtual*

[11] http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/qualitative_study_2008/summary_report_en.pdf

[12] www.virtualglobaltaskforce.com/

Global Task Force). Toutefois, ce n'est pas le cas de tous les enfants. Nous pouvons remarquer que les enfants qui sont conscients des risques se «régulent» eux-mêmes dans leurs activités, mais qu'ils ne partagent souvent pas une vision des nouvelles technologies impliquant que les adultes soient un point de référence pour le jugement et le contrôle du comportement des jeunes[13]. Nous devons faire attention à faire des distinctions simples entre les mondes en ligne et hors ligne, car cela ne reflète plus la façon dont nos vies quotidiennes sont devenues de plus en plus associées aux technologies en ligne. Pour de nombreux enfants, cela signifie une négociation minutieuse entre les opportunités qu'offrent les technologies (comme explorer leur identité, établir des relations proches et augmenter la sociabilité) et les risques (quant à leur vie privée, les incompréhensions et les pratiques abusives) autorisés par la communication dont le support média est Internet[14].

Un même rôle pour tous?

Il est important de se rappeler que pour les enfants et les jeunes, ce sont les enseignants et les parents qui sont les premiers supports d'apprentissage[15].

Le rapport anglais *UK Byron Report*[16] suggère que les politiques de protection des enfants devraient inclure une campagne de sensibilisation soutenant l'apprentissage des adultes (parents, enseignants, tuteurs) qui ne seraient pas à l'aise avec la technologie, ainsi qu'une campagne permettant aux enfants d'avoir des pouvoirs, afin qu'ils soient encouragé sur des sujets tels que des considérations de sécurité et de diminution des prises de risque.

Le bon message aux bonnes personnes

Le principal objectif d'une telle campagne est de modifier les comportements, y compris encourager des comportements en ligne plus sûrs de la part des enfants, encourager une surveillance en ligne effective par les parents et encourager ceux qui interagissent avec des enfants (membres de la famille élargie, enseignants, etc.) afin d'apprendre aux enfants comment rester en sécurité en ligne.

La sécurité des enfants sur Internet ne doit pas être considérée comme un problème isolé, mais plutôt comme un problème ayant des points communs avec un certain nombre d'initiatives concernant les enfants, leur sécurité et Internet.

Le rôle que peuvent jouer les parents et les tuteurs

Pour s'assurer que les enfants utilisent les sites Internet de manière sûre et responsable, les parents et les tuteurs peuvent:

1. Parler à leurs enfants de ce qu'ils font et avec qui ils communiquent lorsqu'ils utilisent leur ordinateur ou un terminal personnel, tel qu'un téléphone mobile ou une console de jeux. Initier et maintenir ce dialogue est crucial pour garder les enfants en sécurité.
2. Lire les termes et conditions d'utilisation avec leurs en-

[13] Quayle, E., Lööf, L. & Palmer, T. (2008), *Child Pornography and Sexual Exploitation Of Children Online*. Bangkok: ECPAT International.
[14] Livingstone, S. *Taking risky opportunities in youthful content creation: teenager's use of social networking sites for intimacy, privacy and self-expression. New Media and Society*, 10 (3), 2008, 393-411.
[15] Livingstone, S., Bober, M., UK *Children Go Online, Final report of key project findings*, avril 2005
[16] Byron, T. (2008), *Safer Children in a Digital World.*

fants avant d'entrer sur le site, discuter ensemble des précautions à prendre en matière de sécurité, définir quelques règles de base et contrôler l'usage pour s'assurer que les règles sont respectées.

3. Eduquer les jeunes utilisateurs à l'usage responsable des technologies en général, les encourager à écouter leur instinct et à utiliser leur bon sens.
4. Vérifier si les sites utilisent des solutions techniques telles que:
   - × Les filtres et contrôles parentaux.
   - × L'historique d'utilisation.
   - × La modération, et si c'est le cas, si elle est effectuée par des humains ou par des moyens automatiques, par exemple à l'aide d'un filtrage du texte, qui va reconnaître des schémas ou groupe de mots spécifiques et des URL? Est-ce que le site utilise une combinaison d'interventions humaines et d'outils techniques? Les modérateurs humains sont entraînés pour assurer un environnement sûr et approprié. Les modérateurs actifs sont souvent décrits comme des personnages ou des participants du monde virtuel ou, dans un contexte de jeu, peuvent agir comme hôte du jeu; dans tous les cas, ils sont clairement visibles de tous les utilisateurs. En général, un modérateur dans le jeu n'interviendra que si une situation difficile se présente, mais dans certains jeux ils vont porter assistance aux utilisateurs qui semblent être «perdus» ou avoir besoin d'aide. Les modérateurs silencieux restent en général en arrière plan, bloquant les éléments offensifs, réagissant lorsqu'ils détectent un comportement suspect, avertissant les utilisateurs et réalisant toute activité de police nécessaire.
   - × Si le site autorise l'envoi de photographies ou de vidéos, est-ce que le site les modère activement ou est-ce qu'il ne visionne que les images qui ont fait l'objet d'un signalement?
   - × Les fonctionnalités de signalement et de blocage: en général sont disponibles des outils de signalement des envois, discussions et activités inappropriés, tels que les boutons de «marquage» ou de «signalisation» d'un abus. Le monde virtuel devrait aussi afficher une politique claire sur la façon de signaler un comportement inapproprié et à qui le faire. Il faudrait apprendre aux enfants comment signaler des incidents ou des contacts indésirables et comment bloquer des contacts indésirables, utiliser les paramètres de confidentialité et enregistrer des conversations en ligne.
   - × Les évaluations: Les parents et tuteurs devraient reconnaître les symboles des évaluations et leur usage comme un outil important de protection des jeunes utilisateurs face aux services et contenus inappropriés.
   - × La vérification de l'âge: Si un site annonce utiliser une vérification de l'âge, quelle est la robustesse des systèmes? Si des produits ayant une limite d'âge sont en vente, est-ce qu'un système fiable de vérification de l'âge est utilisé pour vérifier l'âge de la personne?
5. Rester impliqué dans les activités en ligne des jeunes utilisateurs. Il est crucial de souligner l'importance du rôle que les parents et ceux qui s'occupent des enfants peuvent et doivent jouer dans le cadre des sites Internet, car leur implication a un effet très puissant sur l'expérience de leurs enfants en promouvant les comportements positifs.
6. Rester calme et ne pas tirer de conclusions hâtives si vous entendez ou voyez des choses qui vous concernent à propos du comportement de votre enfant ou de celui de l'un de ses amis en ligne. Certains sites Internet sont des lignes de vie sociales pour certaines jeunes personnes.

Si vos enfants craignent que vous ne leur coupiez tout simplement leur ligne de vie sociale, il est probable qu'ils soient d'autant plus réticents à partager les problèmes ou préoccupations qu'ils pourraient avoir.

7. Être conscient que votre enfant peut se comporter de manière très différente en ligne et hors ligne, en face à face avec vous. Il n'est pas inhabituel que des personnes soient plus agressives en ligne, où elles pensent qu'on ne leur en tiendra pas rigueur. Utiliser tout signalement par votre enfant d'un comportement inapproprié comme une opportunité de discuter avec votre enfant du ton qu'il convient d'adopter lors de communications en ligne.
8. Apprendre la culture en ligne afin d'évaluer l'authenticité des excuses typiques données par les jeunes lorsqu'ils doivent rendre comptes de leur comportement en ligne, comme par exemple «quelqu'un a utilisé mon compte». Ceci est rarement le cas lorsqu'il s'agit de messages et journaux de bord des messageries ayant outrepassé les règles d'un monde virtuel. Cela peut se produire, mais c'est exceptionnel.
9. Apprendre à vos enfants à ne pas partager les mots de passe avec des amis ou des frères et sœurs. Il s'agit de l'un des plus gros problèmes auxquels les sites Internet font face avec les jeunes. Par exemple, un ami, un frère ou une sœur peut voler des objets virtuels pour lequel votre enfant a travaillé dur afin de les obtenir.
10. Utiliser la page de contact des sites web pour partager vos préoccupations et questions. C'est leur travail que de faire en sorte que vous soyez à l'aise avec le site.
11. Ne pas supposer que tout le monde sur Internet en veut à votre enfant. Les statistiques indiquent que le nombre de problèmes hors ligne avec des pédophiles dépasse de beaucoup celui des incidents en ligne. En général, les sites pour enfants peuvent être sûrs et offrir à votre enfant une expérience magnifique, créative, sociale et d'apprentissage, mais uniquement si vous restez impliqué et informé.

Le rôle que peuvent jouer les éducateurs

Il est très important que les éducateurs ne fassent pas d'hypothèses sur ce que les enfants et les jeunes savent ou ne savent pas concernant les problèmes de sécurité en ligne. Il y a de nombreux malentendus concernant Internet et ce qui est approprié ou non. Par exemple, de nombreux adolescents partagent leurs mots de passe et cela est souvent considéré comme un signe de réelle amitié.

L'un des rôles importants des éducateurs est d'apprendre aux enfants et aux jeunes l'importance des mots de passe, comment les garder en sécurité et comment créer un mot de passe efficace.

De même, concernant les problèmes de droits d'auteur, de nombreux adultes sont horrifiés de voir l'apparent manque d'intérêt des jeunes utilisateurs concernant le téléchargement illégal de vidéos ou de musique. La recherche[17] suggère que plutôt que de n'être pas concernés par les droits d'auteur, ce serait plutôt un énorme manque de connaissance de la part des enfants et des jeunes concernant les problèmes de légalité des contenus soumis à des droits d'auteur en ligne. Encore une fois, les éducateurs ont un rôle clair à jouer en expliquant cela à leurs élèves.

Les écoles ont l'occasion de transformer l'éducation et d'aider les élèves pour à la fois atteindre leur potentiel et élever les standards des TIC. Toutefois, il est également important que les enfants apprennent comment être en sécurité lorsqu'ils utilisent ces nouvelles technologies,

[17] *Berkman Center – John Palfrey and Urs Gasser, 2008.*

en particulier les technologies collaboratives du web 2.0, par exemple les sites de réseautage social, qui sont en train de devenir un aspect essentiel de l'apprentissage social productif et créatif. Les éducateurs peuvent aider les enfants à utiliser la technologie de manière sage et sûre en[18]:

1. S'assurant que l'école dispose d'un ensemble de politiques et de pratiques robustes et que leur efficacité est contrôlée et évaluée de manière régulière.
2. S'assurant que tout le monde est au courant de la Politique d'Utilisation Acceptable (*Acceptable Use Policy*, AUP) et de son usage. Il est important d'avoir une AUP qui de plus doit être adaptée à l'âge.
3. Vérifiant que la politique anti-harcèlement et brimade de l'école inclut des références au harcèlement sur Internet et via téléphone ou tout autre équipement mobile, et qu'il existe des sanctions effectives pour ceux qui violent la politique.
4. Désignant un coordinateur sur la sécurité en ligne.
5. S'assurant que le réseau de l'école est sûr et sécuritaire.
6. S'assurant qu'un fournisseur d'accès à Internet accrédité est utilisé.
7. Utilisant un produit de filtrage/contrôle.
8. Fournissant une éducation en matière de sécurité en ligne à tous les enfants et en indiquant où, comment et quand elle sera proposée.
9. S'assurant que tout le personnel (y compris le personnel de soutien) a déjà été correctement formé et que leur formation est mise à jour de manière régulière.
10. Ayant un unique point de contact dans l'école. Et en étant capable de rassembler et d'enregistrer les incidents concernant la sécurité en ligne, ce qui donnera à l'école une meilleure vision des problèmes ou tendances qu'il faut gérer.
11. S'assurant que l'équipe de direction et les responsables de l'école ont une compréhension adéquate du problème de la sécurité en ligne.
12. En faisant faire un audit à intervalle régulier de toutes les mesures concernant la sécurité en ligne.

Les effets sur l'éducation et la psychologie

Les enfants font un usage d'Internet qui a considérablement augmenté au cours des dernières années et qui s'est accompagné d'un intérêt croissant concernant les problèmes de sécurité en ligne. Il y a eu tout au long de l'histoire une panique morale récurrente concernant le danger potentiel des technologies de la communication et c'est particulièrement le cas pour les jeunes femmes. Toutefois, on a rétorqué qu'alors que ces dangers sont en cours d'investigation, il apparaît que très souvent ce n'est pas la technologie elle-même qui est coupable, mais plutôt l'ensemble des enfants utilisant la technologie et les angoisses concernant la perte de contrôle parental[19]. Les éducateurs sont perçus comme ayant un rôle vital dans la promotion et l'assurance de la sécurité sur Internet. Il semble que les parents du monde entier pensent que les écoles

[18] BECTA, *Safeguarding Children Online*, 2009.

[19] Cassell, J. & Cramer M., *High Tech or High Risk: Moral Panics about Girls Online*. In T. McPherson (Ed.) Digital *Youth, Innovation, and the Unexpected. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning*. Cambridge, MA: *The MIT Press*, 2008. 53–76.

devraient avoir un rôle central dans l'éducation des enfants à l'usage de manière sûre des technologies et la coalition *Children's Charities Coalition* a également suggéré que «un guide clair doit être proposé aux écoles sur le sujet de l'usage de manière sûre d'Internet, des courriers électroniques, des espaces de discussions, des sites web des écoles et des logiciels de filtrage et de blocage»[20].

Les premières approches de la sécurité en ligne se sont concentrées sur les solutions techniques, telles que l'usage de logiciels de filtrage, mais plus récemment nous avons assisté à l'augmentation de la mobilité des technologies de l'information, en conséquence de quoi les ordinateurs personnels ne sont plus le seul point d'accès à Internet. Actuellement, un nombre croissant de téléphones mobiles et de consoles de jeux offrent une connexion haut débit et les enfants peuvent accéder à Internet alors qu'ils sont à l'école, à la maison, dans une bibliothèque, un café Internet, une enseigne de restauration rapide, un club de jeunes ou même lors des transports vers l'école dans un moyen de transport public. Les écoles offrent la possibilité de travailler sur Internet, de manière collaborative dans un réseau fermé ou simplement entouré d'autres enfants. Parmi les mesures évidentes on peut citer la mise en place d'une sécurité de réseau efficace, mais il faut aller au-delà de cela. Les enfants peuvent avoir des équipements personnels qui ne sont pas couverts par la protection du réseau et BECTA a fait valoir qu'il fallait mettre l'accent sur la compréhension par tout le monde des risques encourus et agir en conséquence. Ils suggèrent que cela signifie concevoir et mettre en place des politiques de sécurité en ligne qui demandent l'implication d'un grand nombre de groupes d'intérêt. Citons:

1. les chefs d'établissement
2. les directeurs
3. les cadres supérieurs
4. les enseignants
5. le personnel de soutien
6. les jeunes personnes et les parents ou tuteurs
7. le personnel des autorités locales
8. les fournisseurs d'accès à Internet (FAI), les fournisseurs d'accès à l'électronique (FAE), tels que les éditeurs de sites de réseautage social, et les consortium haut débit régionaux, qui travaillent en étroite collaboration avec les FAI et les FAE sur les mesures de sécurité des réseaux.

BECTA a indiqué qu'étant donné que tous ces groupes ont une vision pouvant aider à définir les politiques des écoles, il est important de tous les consulter. Toutefois, avoir simplement des politiques ne suffit pas, et tous ceux qui sont impliqués avec des enfants devraient entreprendre des pratiques actives qui aident les jeunes personnes et le personnel à identifier et à avoir un comportement sûr. En impliquant tous ces groupes depuis le début, tout le monde devrait sentir la pertinence de telles politiques ainsi que la responsabilité personnelle de chacun pour les rendre réelles. Créer un environnement d'apprentissage des TIC sûr se base sur plusieurs éléments importants, parmi lesquels sont compris:

1. une infrastructure de prise de conscience de l'ensemble
2. les responsabilités, politiques et procédures
3. un éventail efficace d'outils technologiques
4. une éducation globale sur la sécurité en ligne
5. un programme pour chacun dans l'établissement
6. un processus d'examen qui contrôle en permanence l'efficacité de ce qui précède [21].

Il faut intégrer cela dans les politiques existantes de sécurité des enfants au sein de l'école, plutôt que le voir comme quelque chose géré de manière indépendante par

[20] *Children's Charities Coalition for Internet Safety (2001) – Working to make the Internet a safer place for kids*. Voir www.communicationswhitepaper.gov.uk/pdf/responses/ccc_internet_safety.pdf

[21] BECTA. *Safeguarding Children Online: A Guide for School Leaders: 2009*. Voir www.becta.org.uk/schools/safety

une équipe chargée des TIC. Cela n'a que peu de sens de penser aux brimades et harcèlement sur Internet ou via téléphones mobiles comme étant un phénomène distinct des brimades et harcèlement dans le monde réel. Toutefois, cela ne signifie pas que la technologie ne représente pas une part importante de la solution en mettant en place:

1. une prévention et une protection contre les virus
2. un contrôle des systèmes pour garder trace de qui a téléchargé quoi, quand cela a été téléchargé et quel ordinateur a été utilisé
3. un filtrage et un contrôle des contenus pour minimiser les contenus inappropriés sur le réseau de l'école.

Il apparaît clairement que les problèmes qui se posent en relation avec les nouvelles technologies ne s'appliquent pas à tous les enfants et que lorsqu'ils se posent, ils dépendent de l'âge des enfants utilisant ces technologies. Fin 2008, le groupe de travail américain sur la sécurité sur Internet (*US Internet Safety Technical Taskforce*) a présenté un rapport intitulé «Améliorer la sécurité des enfants et les technologies en ligne» (*Enhancing Child Safety & Online Technologies*) qui fournit une utile liste de la littérature concernant la recherche originale et publiée sur les sollicitations sexuelles en ligne, le harcèlement et les brimades en ligne, et l'exposition à des contenus problématiques[22]. Il est noté dans ce rapport «qu'il est à craindre que les médias grand public n'amplifient ces peurs, les rendant disproportionnées par rapport aux risques auxquels les jeunes font face.

Cela crée le danger d'obscurcir les risques connus, réduit la probabilité que la société s'intéresse aux facteurs conduisant aux risques connus et par inadvertance nuit souvent aux jeunes de manière inattendue». La couverture média des crimes via Internet commis à l'encontre des enfants semble souvent faire écho aux positions polarisées des professionnels et des universitaires qui travaillent dans ce domaine, avec un pendule oscillant entre ceux qui pensent qu'il existe un danger de distorsion des menaces qui pèsent sur les enfants, et ceux pour qui la menace a été largement sous-estimée.

[22] ISTTF (2008), *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force To the Multi-State Working Group on Social Networking of State Attorneys General of the United States.* Harvard University: The Berkman Center for Internet and Society.

Toutefois il existe une crainte que la technologie Internet médiatisée puisse rendre quelques enfants vulnérables et que les éducateurs, ainsi que les parents et tuteurs, ont une responsabilité par rapport à cela. Nous savons étonnamment peu de chose concernant la manière dont les enfants deviennent victimes de violences et les facteurs qui améliorent la résilience. Les formes de victimisation comprennent:

1. La sollicitation ou grooming (manipulation psychologique) des enfants

2. L'exposition à du matériel problématique ou illégal

3. Le harcèlement en ligne

Une manière utile de réfléchir aux risques est décrite dans le tableau suivant[23:]

	Commercial	Agressif	Sexuel	Valeurs
Contenu (enfant destinataire)	Publicités spam, parrainage, informations personnelles	Contenu violent/ haineux	Contenu pornographique ou sexuel importun	Informations et avis biaisés, racistes ou trompeurs
Contact (enfant participant)	Recherche/ collecte d'informations personnelles	Être intimidé, harcelé ou faire l'objet de chantage	Rencontrer des inconnus ou être manipulé psychologiquement	Automutilation ou persuasions importunes
Animation (enfant acteur)	Téléchargement illégal, piratage informatique, jeux d'argent, escroqueries financières ou terrorisme	Intimider ou harceler une autre personne	Créer et mettre en ligne des données inappropriées	Fournir des informations et avis trompeurs

[23] Tableau développé par le projet EUKids Online et référencé dans le paragraphe 1.3 du Byron Review

Sollicitation et *grooming* (manipulation psychologique) en ligne

Dans le contexte de sollicitation sexuel ou de *grooming*, nous comprenons mieux le processus de victimisation, en partie car la recherche a largement impliqué les enfants eux-mêmes.

Une bonne partie de cette recherche provient du centre de recherche des crimes contre les enfants (*Crimes against Children Research Centre*, CCRC) de l'Université du New Hampshire et a été initiée par deux études (YISS-1 et YISS-2), qui impliquent des entretiens téléphoniques avec un échantillon national de jeunes utilisateurs d'Internet âgés de 10 à 17 ans, et réalisés de 2000 à 2005. Il est fait également d'autres références à ce sujet dans l'étude *International Youth Advisory Council Global Online Survey*[24, 25, 26].

Ces chercheurs ont récemment suggéré que leur travail concernant les crimes sexuels initiés sur Internet rend évident que le stéréotype de l'agresseur d'enfants sur Internet utilisant ruse et violence pour attaquer les enfants est largement inexact[27].

Cette étude américaine suggèrerait plutôt que la plupart des crimes sexuels initiés sur Internet impliquent des hommes adultes utilisant Internet pour rencontrer et séduire des adolescents mineurs afin de faire des rencontres sexuelles.

Les délinquants utilisent les communications via Internet, telles que les messageries instantanées, les courriers électroniques, les salons virtuels (*chatrooms*) pour rencontrer et développer des relations intimes avec les victimes.

Leur travail indique que dans la majorité des cas, les victimes sont conscientes de discuter en ligne avec des adultes.

Jusqu'à présent, l'accent a été porté sur les enfants qui font l'objet de pratiques abusives, en ignorant le type de monde social et culturel que les jeunes créent en ligne.

Toutefois, les enfants et les adolescents ne sont pas simplement les cibles de créations des adultes sur Internet, mais sont des participants actifs de la création de leur propres cybercultures.

Les études de l'Université du New Hampshire soulignent que ce sont ces aspects d'Internet qui créent les risques pour certaines jeunes personnes qui s'engagent dans des comportements spécifiques avec les nouvelles technologies.

Alors que la majorité des jeunes semblent *prendre des risques* (et en particulier les garçons plus âgés), la vaste majorité des enfants ne semblent pas *courir de risques*[28].

Toutefois, les jeunes qui envoient des informations personnelles (par exemple, nom, numéro de téléphone, photographies) à des inconnus ou discutent en ligne avec ces personnes à propos de sexe sont plus susceptibles de faire l'objet de sollicitations sexuelles agressives, impliquant des contacts hors ligne réels ou tentés.

Au cours des cinq ans séparant YISS-1 et 2, il y a eu une baisse générale du nombre de sollicitations sexuelles, toutefois cela n'a pas été observé parmi les jeunes issus des minorités et des familles les moins aisées.

Les auteurs ont le sentiment que l'augmentation du harcèlement est largement expliquée par l'augmentation de l'usage d'Internet au cours de la période de cinq ans.

Toutefois, en 2005 les jeunes étaient 1,7 fois plus susceptibles de signaler des sollicitations agressives, même si l'on ajuste les chiffres par rapport aux modifications démographiques et d'usage d'Internet et de ses caractéristiques.

---

24 Finkelhor, D., Mitchell, K. and Wolak, J. *Online victimization: A report on the nation's youth.* (NCMEC 6-00-020). Alexandria, VA: *National Center for Missing and Exploited Children.* 2000.

25 Wolak, J. Mitchell, K. and Finkelhor, D. *Online victimization: 5 year later* (NCMEC 07-06-025). Alexandria, VA: *National Center for Missing and Exploited Children.* 2006.

26 www.virtualglobaltaskforce.com/iyac_charter_supp.pdf

27 Wolak, J., Finkelhor, D., Mitchell, K.J., and Ybarra, M.L. Online «predators» and their victims. American Psychologist, 63 (2), 2008, 111-128.

28 OPTEM. *Safer Internet for Children. Qualitative Study in 29 European Centres.* Bruxelles: Commission Européenne, 2007.

Les facteurs de risque identifiés pour ces sollicitations agressives comprennent être une femme, utiliser des salons de discussion virtuels (*chatrooms*), utiliser Internet mobile, parler à des personnes rencontrées pour la première fois en ligne, envoyer des informations personnelles à des personnes rencontrées pour la première fois en ligne, et faire l'expérience d'abus physiques et sexuels hors ligne.

Dans la deuxième étude, 4% (65 cas) ont signalé une demande en ligne d'envoi d'une image sexuelle d'eux-mêmes au cours de l'année écoulée, mais seule une jeune personne l'a réellement fait.

Être une femme, d'ethnicité afro-américaine, ayant une relation étroite, s'engageant en ligne dans un comportement sexuel et faisant hors ligne l'expérience d'abus sexuel ou physique étaient des facteurs de risque pour recevoir une demande d'image sexuelle.

Il est intéressant de noter que les demandes étaient plus susceptibles d'être faites lorsque les jeunes étaient avec des amis, communiquant avec un adulte, quelqu'un qu'ils avaient déjà rencontré en ligne, qui avait déjà envoyé une image sexuelle aux jeunes et qui avaient déjà tenté ou réussi à établir une certaine forme de contact hors ligne[29].

Dans la première étude les sollicitations sexuelles semblaient être associées à des signes de dépression[30].

Les jeunes affichant les principaux symptômes de ce qui semblait être une dépression étaient 3,5 fois plus susceptibles de signaler une sollicitation sexuelle importune en ligne par rapport à ceux qui avaient de légers, voire aucun symptômes, et ceux qui avaient des symptômes étaient deux fois plus susceptibles d'indiquer être en détresse émotionnelle suite à l'incident.

En général, la détresse était plus commune chez les plus jeunes, ceux qui avaient reçu des sollicitations agressives et ceux qui avaient été sollicités sur un ordinateur hors de leur domicile[31].

Une étude suédoise récente a examiné le nombre de jeunes de 16 ans qui avaient reçu des demandes de rencontres sexuelles en ligne et hors ligne.

Parmi les 7449 réponses, 46% des filles ont indiqué avoir reçu de telles requêtes de la part d'un adulte.

Plusieurs personnes ayant répondu ont signalé avoir reçu de telles sollicitations à la fois via Internet et via d'autres moyens.

Le chiffre correspondant aux garçons étaient de 16%. Les demandes aux adolescents consistaient en se déshabiller devant la webcam ou regarder un adulte pendant qu'il se masturbait devant sa webcam.

Les adolescents de l'étude ont décrit ces incidents comme communs et arrivant tout le temps lorsque l'on utilise les sites de discussion.

Aucune des tentatives de sollicitations décrites n'étaient le moins du monde sophistiquées; l'adulte a commencé à demander des services sexuels dès le début de la conversation virtuelle.

Dans la même étude, les signalements à la police de crimes à l'encontre d'enfants commis via de nouvelles technologies ont été examinés et dans 50% d'entre eux, les crimes signalés n'ont lieu qu'en ligne où les demandes d'images ou de contacts via webcam sont les plus fréquentes.

Les autres crimes signalés étaient des infractions commises hors ligne, mais pour lesquelles le premier contact avait été établi par Internet.

Dans la moitié des crimes hors ligne, la victime a rencontré l'auteur en sachant que la rencontre amènerait à du sexe.

Les autres crimes étaient tous des crimes dans lesquels la victime pensait que la rencontre serait d'une toute autre nature[32].

---

29 Mitchell, K.J., Finkelhor, D. et Wolak, J. *Youth Internet users at risk for the most serious online solicitations. American Journal of Preventive Medicine*, 32 (6), 2007, S32-S37.

30 Ybarra, M.L., Leaf, P.J. et Diener-West, M. *Sex differences in youth-reported depressive symptomatology and unwanted Internet sexual solicitation. Journal of Medical Internet Research*, 6 (1), 2001, 9-18.

31 Mitchell, K.J., Finkelhor, D. et Wolak, J. *Risk factors for and impact of online sexual solicitation of youth*. JAMA, 285 (23), 2001, 3011-3014.

32 Brottsförebyggande Rådet. *Vuxnas sexualla kontakter med barn via Internet*. [Rapports sexuels entre adultes et enfants par l'intermédiaire de l'Internet], Rapport 2007:11. Brottsförebyggande Rådet. 2007. Stockholm.

Les chiffres récents des victimes de sollicitation ou de *grooming* en Suède, ont à la fois confirmé et infirmé les découvertes de l'étude du New Hampshire.

Dans une affaire suédoise d'importance impliquant plus de 100 filles, il fut évident que toutes les jeunes filles savaient qu'elles allaient rencontrer un homme qui voulait avoir une relation sexuelle avec elles. En même temps, aucune des jeunes filles ne voulaient admettre qu'elles étaient pleinement conscientes de ce que cela impliquait.

Quelque chose dans les conversations virtuelles avec les jeunes filles signalait à l'auteur leurs vulnérabilités et lui donnait l'occasion d'exploiter ces faiblesses, et ce bien avant d'exploiter sexuellement les jeunes filles.

Les vulnérabilités allaient de la solitude aux pensées suicidaires.

Le fait que les jeunes filles aillent d'elles-mêmes aux rendez-vous avec l'auteur n'en faisait pas des sujets consentants[33].

Il est évident que le nombre de sollicitations pour des contacts en ligne est significatif et que les enfants et les adolescents signalent lorsqu'ils se produisent, et que tous les enfants en sont conscients.

En examinant les cas dans lesquels les infractions ont été commises à la fois en ligne et hors ligne, il apparaît clairement que les demandes faites aux adolescents d'envoyer des images ou de faire des actes sexuels devant la caméra sont le point de départ de l'abus sexuel.

Au cours des dernières années, les préoccupations ont augmenté quant aux types de comportements en relation avec les sites de réseautage social pouvant être associés avec les enfants se mettant eux-mêmes en danger.

Nous aborderons ce point plus en détail lorsque nous examinerons les opportunités fournies par Internet aux jeunes de s'engager dans des comportements problématiques, mais il est intéressant de noter que dans l'étude YISS-2, 16% des enfants ont indiqué avoir utilisé des blogs dans l'année écoulée.

Les blogs contiennent des données créées par les utilisateurs d'Internet et partagent certaines des qualités des sites de réseautage social.

Toutefois, il a été démontré que les adolescents et les filles sont les blogueurs les plus fréquents et que les blogueurs sont plus susceptibles que les autres jeunes de poster des informations personnelles en ligne[34].

Toutefois, les blogueurs ne sont pas plus susceptibles d'interagir avec des personnes rencontrées pour la première fois en ligne et qu'ils ne connaissent pas personnellement.

Les blogueurs qui n'interagissent pas n'ont pas plus de risques de sollicitations sexuelles et poster des informations personnelles en elles-mêmes, et les concernant eux-mêmes, n'augmente pas leurs risques.

Toutefois, les blogueurs ont plus de risques de harcèlement en ligne, peu importe qu'ils interagissent en ligne avec d'autres personnes ou non.

L'étude *UK Children Go Online Survey* suggère également que les jeunes les moins satisfaits de leur vie et étant devenus des utilisateurs d'Internet plus fréquents et expérimentés, sont plus susceptibles de considérer Internet comme un environnement communicatif, qui peut conduire à des comportements risqués[35].

L'expérience et la pratique permettent de mettre en évidence un certain nombre de facteurs qui doivent évoluer si nous voulons pouvoir aider les enfants victimes de grooming en ligne en vue d'abus sexuel hors ligne.

Nous avons appris que la manipulation psychologique, le *grooming* en ligne, par rapport au *grooming* hors ligne, se produit plus rapidement et peut être anonyme: les enfants font plus rapidement confiance à leurs «amis» en ligne et tendent à être

33 Wagner, K: *Alexandramannen*. Förlags AB Weinco. Västra Frölunda. 2008.

34 Mitchell, K.J., Wolak, J. et Finkelhor, D. *Are blogs putting youth at risk for online sexual solicitation or harassment? Chid Abuse and Neglect*, 32, 2008, 277-294.

35 Livingstone, S. et Helsper, E.J. *Taking risks when communicating on the Internet. The role of offline social-psychological factors in young people's vulnerability to online risks. Information, Communication and Society*, 10 (5), 2007, 618-643.

moins inhibés dans ce qu'ils communiquent, et de tels délinquants ne sont pas limités par le temps ou l'accessibilité comme ils le seraient dans le monde «réel».

En général, les auteurs en apprennent autant que possible sur leur victime potentielle; ils établissent les risques et probabilité que l'enfant raconte tout; ils découvrent quels sont les réseaux sociaux de l'enfant; ils peuvent donner de fausses informations les concernant, y compris de fausses images et s'ils sont suffisamment en sécurité ils vont créer une «relation» avec l'enfant ou le contrôler de telle manière qu'ils puissent le rencontrer hors ligne[36].

Les approches thérapeutiques aidant les enfants ayant été victimes d'exploitation en ligne et hors ligne sont en cours d'investigation au BUP Elefanten, qui est une unité psychiatrique pour enfants et adolescents traitant des enfants abusés sexuellement et physiquement en Suède.

Le projet avance depuis 2006, et a impliqué plus de 100 entretiens avec des jeunes, des thérapeutes, des policiers, des procureurs et des travailleurs sociaux.

Ces jeunes ont subi des pratiques abusives diverses, comprenant: le harcèlement sexuel, des actes sexuels devant une webcam, le téléchargement d'images d'eux sur Internet, l'engagement en ligne menant à l'abus hors ligne et la vente par les enfants de sexe en ligne[37].

L'analyse de ces données issues des entretiens suggère que ces jeunes peuvent être divisés en trois groupes descriptifs:

1. ceux qui ont été dupés et qui ont été attirés dans une situation à laquelle ils ne s'attendaient pas;
2. ceux qui prennent des risques pour satisfaire des besoins émotionnels et s'assurer une attention;
3. ceux qui sont auto-destructeurs, qui par exemple vendent du sexe ou s'engagent consciemment dans des relations abusives.

Les membres du dernier groupe répugnent à se voir comme des «victimes», ils se positionnent plutôt comme ayant le contrôle sur la situation.

Les résultats de ces découvertes cliniques suggèrent que nombre de ces enfants rejettent l'aide qui leur est offerte, et il est important que les praticiens n'abandonnent pas ces enfants, mais plutôt qu'ils tentent de garder le contact avec eux jusqu'à ce qu'ils se sentent prêts à se lancer dans des méthodes d'aide ou d'intervention.

L'un des impacts prédominants du processus de *grooming* chez les enfants, qui deviennent les sujets d'images abusives, est de les réduire au silence.

Ce silence est amené à la fois par le fait que les jeunes croyaient sincèrement que la personne qu'ils allaient rencontrer était leur amie et qu'ils ne veulent pas que soit divulguées les conversations qu'ils ont eu en ligne.

Le premier point a des implications sur le façon dont les jeunes définissent et déterminent les amitiés, le deuxième a trait au fait que, comme indiqué ci-dessus, les jeunes sont devenus bien moins inhibés dans leurs communications en ligne.

[36] Palmer, T. *Just One Click*. Londres: Barnardos. 2004.

[37] Quayle, E., Lööf, L. & Palmer, T. (2008). *Child Pornography And Sexual Exploitation Of Children Online*. Bangkok: ECPAT International.


“Internet emmène les enfants et les jeunes virtuellement n’importe où dans le monde – et dans le processus ils peuvent être exposés à des risques potentiellement dangereux.”

Accéder à des données problématiques en ligne

Alors qu'il serait naïf de croire que les données pornographiques ou sexuelles n'existaient pas avant Internet, il est vrai de dire qu'Internet a apporté la prolifération de données sexuelles facilement accessibles.

L'accessibilité, l'interactivité et l'anonymat d'Internet, toutefois, sont les facteurs mêmes qui augmentent la probabilité d'exposition aux données violentes ou sexuelles.

D'après l'étude SAFT, 34% des enfants ont vu un site web violent, soit accidentellement, soit à dessein[38].

Les études du New Hampshire ont mis en lumière l'exposition accidentelle des jeunes aux données sexuelles importunes sur Internet, mais ont reconnu le fait que les recherches existantes examinant les effets d'une telle exposition à des données sexuelles non souhaitées se sont largement concentrées sur des étudiants ou de jeunes adultes plutôt que sur des enfants, et sur les expositions volontaires plutôt qu'accidentelles.

On suppose que les différents types d'adolescents qui sont pris dans des relations en ligne abusives et d'exploitation peuvent indiquer que les jeunes qui prennent des risques ou sont auto-destructeurs peuvent également accéder à de la pornographie ou visiter des sites de discussion destinés aux adultes recherchant des partenaires sexuels, mais peu de recherche étaye cela.

L'étude YISS-1 indique qu'un enfant sur quatre utilisant régulièrement Internet a vu des images sexuelles non souhaitées dans l'année précédant la collecte des données. 73% de telles expositions ont eu lieu alors que les enfants cherchaient quelque chose ou surfaient sur Internet, et la majorité des cas a eu lieu à la maison, plutôt qu'à l'école.

Ces auteurs ont également abordé la manière dont les techniques de programmation maintiennent de telles expositions, rendant difficile d'en sortir. Une telle «prise au piège» s'est produite dans un tiers des incidents pénibles.

La majorité des enfants exposés aux données n'ont pas considéré cette exposition comme étant particulièrement pénible.

Toutefois, les auteurs ont souligné qu'une telle exposition, en particulier non souhaitée, peut affecter les attitudes concernant le sexe, Internet et la sensation de sécurité et de communauté des jeunes.

Selon l'étude YISS-2, il y a eu une augmentation des expositions importunes à la pornographie et cela est particulièrement flagrant parmi les 10-12 ans, les garçons de 16-17 ans et les jeunes blancs, non-hispaniques[39].

Selon une étude sur les jeunes Australiens (16-17 ans), les trois quarts d'entre eux avaient été exposés accidentellement à des sites web pornographiques, alors que 38% des garçons et 2% des filles y avaient eu accès délibérément[40].

Cette étude a conclu que deux traits de l'exposition des enfants à la pornographie sont le reflet de celle des adultes.

En premier lieu, les hommes ont plus tendance à chercher et à être des clients de films classés X et de sites pornographiques.

Ensuite, les utilisateurs d'Internet de tous âges trouvent qu'il est difficile d'éviter les rencontres impor-

---

38 SAFT. Safety *Awareness Facts Tools*. Bruxelles: Commission Européenne. dernière visite le 5.6.2007. http://ec.europa.eu/information_society/activities/sip/projects/awareness/closed_projects/saft/index_en.htm.

39 Mitchell, K.J., Wolak, J. et Finkelhor, *D. Trends in youth reports of sexual solicitations, harassment, and unwanted exposure to pornography on the Internet. Journal of Adolescent Health*, 40, 2007, 116-126.

40 Flood, M. *Exposure to pornography among youth in Australia. Journal of Sociology*, 43 (1), 2007, 45-60.

tunes avec des données explicitement sexuelles.

Par exemple, certains jeux sur ordinateur peuvent avoir une grande composante sexuelle. De tels jeux ont beau être classés «pour adultes», la participation des jeunes est particulièrement élevée.

Il est également important de noter qu'une telle exposition n'est pas spécifique aux nouvelles technologies, mais prend également place dans des médias plus traditionnels tels que la télévision, où l'heure de diffusion de vidéos érotiques et sexuelles peut coïncider avec celle où les enfants sont susceptibles de regarder la télévision.

L'un des facteurs pouvant être d'importance ici se rapporte à la contrôlabilité des expositions, et il est possible qu'il existe des différences dans l'impact d'une exposition accidentelle et d'une exposition réfléchie.

Il a également été découvert qu'il existe un certain nombre de mineurs qui sont surpris par le contenu de certains matériaux sur lesquels ils tombent par inadvertance lorsqu'ils utilisent Internet[41]. L'accès imprévu ou partiel au matériau peut être un problème important et il a été suggéré que[42]: «Les nouvelles technologies (y compris la vidéo, mais également Internet et les communications mobiles) autorisent une visualisation hors contexte des contenus.

On peut voir des ensembles de bandes-annonces plutôt que l'action en entier pour comprendre le contenu. Le contexte éditorial a toujours été important pour les lignes directrices de la réglementation des contenus (par exemple, BBFC, Ofcom), qui peuvent s'avérer difficiles à transformer en lignes directrices parallèles pour un nouveau média.

Toutefois, il est clair d'après la recherche sur l'exposition accidentelle des enfants à la pornographie sur Internet que le contenu inattendu et sorti de son contexte peut être particulièrement bouleversant. Ce qui crée un défi pour les régulateurs».

Toutefois, l'usage de la pornographie par les jeunes n'a pas été largement étudié et est essentiellement basé sur des signalements, dans lesquels les différences peuvent très bien être celles que la norme sociétale prévalente dicterait aux adolescents.

On peut faire valoir que de nombreux enfants et adolescents vont prétendre n'être tombé que par hasard sur de la pornographie car ils pensent qu'il n'est pas approprié d'indiquer qu'ils l'ont recherchée activement sur Internet.

Dans un échantillon suédois de jeunes de 18 ans, 65% des garçons visionnent de la pornographie tous les mois, contrairement aux 5% de filles. Il faut noter que seuls 7% des garçons et 31% des filles de l'étude ont indiqué n'avoir jamais vu de pornographie[43].

De nombreux jeunes sont exposés à des matériaux sexuels en ligne, et nous avons clairement vu que toutes ces expositions ne sont pas accidentelles ou dommageables.

L'une des préoccupations est que l'exposition à de la pornographie déviante ou violente puisse avoir un impact sur les croyances et les attitudes de certains jeunes, et dans une moindre mesure sur le comportement de quelques uns.

Ceci est vu de manière croissante comme un problème de santé publique potentiel, et il apparaît que les conséquences de cette exposition au sein du médium largement non-régulé qu'est Internet méritent certainement de plus amples recherches[44].

---

41 Fug, O.C. *Save the children: The protection of minors in the information society and the audiovisual media services directorate. Journal of Consumer Policy*, 31, 2008, 45-61.

42 Livingstone, S. et Hargrave, A.M. *Harmful to children? Drawing conclusions from empirical research on media effects*. In U. Carlsson (ed) *Regulation, Awareness, Empowerment. Young People and Harmful Media Content in the Digital Age*. Göttenborg: Nordicom. 2006.

43 Mossige, S., Ainsaar, M. et Svedin, C.G. *The Baltic Sea Regional Study on Adolescent´s Sexuality*. NOVA Rapport 18/07. Oslo: NOVA, s. 93-111

44 Perrin, P.C., Madanat, H.N., Barnes, M.D., Corolan, A., Clark, R.B., Ivins, N. et al. *Health educationa's role in framing pornography as a public health issue: local and national strategies with international implications. Promotion and Education*, 15, 2008, 11-18.

Opportunités problématiques

Un danger supplémentaire lié aux nouvelles technologies vient du média lui-même et des opportunités offertes aux jeunes de se livrer à des comportements qui pourraient être jugés dignes d'intérêt.

Ces activités peuvent être appelées activités d'auto-victimisation par le biais à la fois d'Internet et des technologies des téléphones mobiles, bien que ce terme puisse être considéré comme problématique, car il est largement lié à la faculté de générer du contenu en ligne.

L'évidence suggèrerait que la possession de téléphones mobiles peut être plus élevée parmi les enfants de 11-16 ans que parmi les adultes, les enfants ayant pour 76% d'entre eux leur propre téléphone mobile[45].

Une étude portant sur 1340 enfants au lycée dans la zone de Teesside en Royaume Uni en 2004 a montré que 86% d'entre eux possédaient un téléphone mobile (89,7% pour les filles, 82,3% pour les garçons)[46].

Dans cette étude, l'usage des téléphones mobiles était limité à la voix et au texte, mais il est évident que les téléphones mobiles peuvent de plus en plus servir à d'autres formes de communication.

Dans l'étude *UK Children Go Online*, toutefois, il apparaît que cela se diversifie maintenant et que 38% des jeunes disposent d'un téléphone mobile, 17% d'une télévision numérique et 8% d'une console de jeu, tous ayant accès à Internet.

Pour de nombreux jeunes, le téléphone mobile est à la fois un moyen vital de communication et un moyen d'être en relation et

[45] *Child-Wise Monitor* (2002). Dernière visite le 18.06.07. www.childwise.co.uk/monitor.htm

[46] Madell, D. et Muncer, S. *Back from the beach but hanging on the telephone? English adolescents' attitudes and experiences of mobile phones and the Internet. CyberPsychology and Behavior*, 7 (3). 2004, 359-367.

de participer à un monde social étendu.

En 2007, l'étude qualitative de l'OPTEM de 29 pays européens a indiqué que la grande majorité des enfants disposaient de téléphones mobiles.

Toutefois, des préoccupations émergent selon lesquelles la participation technologique implique des pratiques qui ciblent d'autres individus ou incluent les jeunes eux-mêmes.

Les images ou films autoproduits peuvent être considérés comme éléments du processus de *grooming* dans lequel l'agresseur convainc l'enfant de lui envoyer des images de lui-même ou d'elle-même, soit dénudé(e), soit le représentant ayant un comportement sexuel.

Les images sont souvent utilisées pour persuader l'enfant de l'innocuité des contacts sexuels entre un enfant et un adulte, réduisant l'inhibition de l'enfant à s'engager dans du sexe hors ligne, ou à être payé par l'adulte pour le rencontrer.

L'enfant ciblé est vulnérable pour un certain nombre de raisons, comme la solitude, le fait d'être intimidé ou en bataille constante avec ses parents. L'adolescent impliqué se voit comme un complice de l'abus après avoir envoyé des images à l'auteur.

La question du préjudice a également été examinée par l'Université du New Hampshire à travers l'examen des charges de 1504 praticiens pour voir quels types d'expériences problématiques ont été signalés en relation avec les nouvelles technologies.

Ils ont trouvé onze types d'expériences problématiques signalées à la fois par des clients jeunes et adultes.

Ce sont: la surexploitation, la pornographie, l'infidélité, l'exploitation et l'abus sexuels, le jeu, les paris et jeux de rôle, le harcèlement, l'utilisation menant à l'isolation et l'évitement, les fraudes, le vol et la tromperie, les échecs de relations en ligne, les sites web à l'influence néfaste, et l'utilisation risquée et inappropriée[47].

Une analyse plus approfondie a examiné quelles expériences problématiques ont été identifiées comme des problèmes primaires ou secondaires[48].

Les utilisateurs jeunes et adultes étaient plus susceptibles d'avoir des problèmes en relation avec la surexploitation d'Internet, l'usage de pornographie adulte, de pornographie infantile, la perpétration d'exploitation sexuelle, et le jeu, les paris et les jeux de rôle.

D'autres problèmes liés à Internet, tels que l'utilisation menant à l'isolation et l'évitement, la victimisation et l'exploitation sexuelle, la perpétration de harcèlement et l'infidélité en ligne étaient tous aussi probables.

Les problèmes des jeunes liés au jeu, aux paris et jeux de rôle avaient 1,7 fois plus de chances d'être identifiés comme présentant un problème et la fraude en ligne ou la victimisation et tromperie étaient quatre fois plus probables.

Les jeunes sexuellement exploités étaient plus susceptibles d'avoir un diagnostique de syndrome de stress post-traumatique (SSPT) que les jeunes ayant eu d'autres problèmes liés à Internet.

L'intimidation

Nous avons déjà mentionné que l'intimidation dans le monde virtuel ne doit pas être considérée comme quelque chose de différent de ce qui est vécu dans le monde réel. Les personnes font parfois référence aux harcèlement et brimades en ligne ou via téléphones mobiles sous le l'appellation cyber-harcèlement, mais cela peut ne pas aider tout le monde à comprendre

[47] Mitchell, K.J., Becker-Blease, K.A. et Finkelhor, D. *Inventory of problematic Internet experiences encountered in clinical practice. Professional Psychology: Research and Practice*, 36 (5), 2005, 498-409.
[48] Mitchell, K.J. et Wells, M. *Problematic Internet experiences: Primary or secondary presenting problems in persons seeking mental health care? Social Science and Medicine*, 65, 2007, 1136-1141.

ce qui se passe réellement. Le harcèlement est du harcèlement quel que soit le lieu et la façon dont cela se produit.

L'étude *Byron Review* au Royaume Uni suggère que «le cyber-harcèlement fait référence aux comportements de harcèlement qui ont lieu par le biais de moyens électroniques, tels qu'envoyer des messages textuels de menace, poster des choses déplaisantes sur des personnes, et faire circuler des photographies ou des vidéos désagréables sur quelqu'un».

Le harcèlement en ligne ou via téléphones mobiles peut être une extension du harcèlement et des brimades en face à face, ou cela peut être une forme de représailles pour des incidents hors ligne. Le harcèlement en ligne ou via téléphones mobiles peut être particulièrement bouleversant et dommageable, car sa portée est plus grande, la publicité était plus grande, et le contenu circulant électroniquement peut refaire surface à tout moment, ce qui complique l'obtention de la clôture de l'incident par la victime du harcèlement; il peut contenir des images visuelles dommageables ou des mots blessants; le contenu est disponible 24 heures par jour; le harcèlement électronique peut se produire 24h/24 et 7j/7, il peut donc envahir la vie privée de la victime, même dans des endroits normalement «sûrs» tels que sa maison; et les informations personnelles peuvent être manipulées, les images visuelles modifiées, puis être transmises à d'autres personnes.

En outre, cela peut se faire de façon anonyme[49].

Une telle activité de harcèlement et de brimades peut inclure à la fois des comportements de vexation et des activités très agressives, et les études de l'Université du New Hampshire ont suggéré qu'il y a un grand recouvrement entre les actes illégaux, tels que le harcèlement sexuel, et le harcèlement scolaire.

[49] Byron, T. (2008). *Safer Children in a Digital World. The Report of the Byron Review.* Disponible sur www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf

Une étude allemande récente a étudié les perspectives des victimes de harcèlement dans les salons de discussion virtuels[50].

Ils ont identifié différents types de harcèlement qui incluent le harcèlement, l'abus, les insultes, les vexations et le chantage.

Un tel harcèlement était fréquent et ce sont souvent les mêmes enfants qui sont ciblés.

L'étude a également montré qu'il y avait une corrélation entre les expériences de victimisation à l'école et dans les salons de discussion sur Internet.

Les adolescents qui étaient harcelés à l'école étaient également plus susceptibles de faire l'expérience d'une victimisation dans les salons de discussion virtuels.

Ces enfants étaient également plus susceptibles d'être considérés comme moins populaires, ayant une estime de soi plus faible et ayant des parents plus susceptibles d'être sur-protecteurs.

L'étude a également suggéré que ces enfants évoluent de victimes à intimidateurs et que cela peut être interprété comme «rendre les coups» ou «lâcher du lest».

Les victimes de harcèlement dans les salons de discussion sur Internet ont également souvent signalé consulter des sites en ligne risqués et peuvent en effet se mettre dans des situations dans lesquelles une victimisation est plus probable.

L'étude a indiqué que, par comparaison avec d'autres victimes d'important harcèlement scolaire, les victimes d'important harcèlement dans les salons de discussion affichent plus fréquemment un comportement de manipulation sociale lorsqu'elles consultent des salons de discussion virtuels (par exemple, en donnant de fausses informations concernant leur âge et leur sexe).

La recherche menée avec des enfants Américains a conduit aux conclusions suivantes:

1. Pour les grands utilisateurs d'Internet, le cyber-harcèlement est une expérience commune.
2. Les formes de harcèlement scolaire et en ligne sont similaires et les expériences se chevauchent dans les deux contextes.
3. Bien que certains moyens et équipements de communication électronique soient associés à un risque élevé de «cyber-harcèlement», ils ne sont que des outils, et non les causes des comportements méchants.
4. Indépendamment du harcèlement scolaire, le cyber-harcèlement est associé à une détresse accrue.
5. Les jeunes ne parlent que rarement aux adultes de leurs expériences de harcèlement en ligne et ne profitent pas au maximum des outils fournis par les technologies de communication pour se prémunir contre de futurs incidents.[51]

[50] Katzer, C., Fetchenhauer, D. et Belschak, F. *Cyberbullying: Who Are the Victims? A Comparison of Victimization in Internet Chatrooms and Victimization in School. Journal of Media Psychology,* 2009; Vol. 21(1):25–36.

[51] JUVONEN, J. & Gross, G.F. *Extending the School Grounds?—Bullying Experiences in Cyberspace. Journal of School Health*, 2008, 78 (9), 496 – 505.

4. Lignes directrices pour les parents, tuteurs et éducateurs

Les conseils de sécurité partent de l'analyse des données recueillies et de la recherche disponible. Cette section du document est destinée à fournir, dans un endroit pratique, des lignes directrices pour les parents, tuteurs et éducateurs afin de les aider à apprendre à leurs enfants à avoir une expérience en ligne qui soit sûre, positive et de valeur.

Les parents, tuteurs et éducateurs doivent prendre en considération la nature exacte des différents sites, la compréhension de leurs enfants des dangers et la probabilité que les parents réussissent à réduire les risques, avant de décider quel environnement convient à leur enfant.

Internet a un grand potentiel en tant que moyen permettant aux enfants et aux jeunes de trouver des informations par eux-mêmes. Leur apprendre les formes de comportement en ligne positives et responsables est un objectif essentiel.

Parents, tuteurs et éducateurs			
	#	Domaines essentiels à considérer	Description
Sûreté et sécurité de votre ordinateur personnel	1.	Gardez l'ordinateur dans une pièce commune	Garder l'ordinateur dans une pièce commune et être présent en particulier lorsque les enfants les plus jeunes utilisent Internet peut être très important. Si vous ne pouvez pas être présent, envisagez d'autres moyens de garder une surveillance rapprochée de ce que vos enfants font en ligne, par exemple en utilisant des outils techniques. Dans les grandes familles disposant de plusieurs ordinateurs, il se peut qu'il y ait des limites pratiques qui apparaissent si vous insistez sur le fait de garder tous les ordinateurs dans la même pièce au même moment, et rappelez-vous que les enfants grandissant ont de toute façon droit à un peu de confidentialité. Etant donné que de plus en plus d'enfants disposent d'un ordinateur portable et que les maisons sont de plus en plus équipées de réseaux sans fils, il sera plus difficile de maintenir une règle de ce type.
	2.	Installez des logiciels antivirus et pare-feu	Assurez-vous que votre ordinateur a des logiciels anti-virus et pare-feu installés et qu'ils sont à jour. Apprenez à vos enfants les bases de la sécurité sur Internet.
Règles	3.	Définissez des règles domestiques concernant l'usage d'Internet et des terminaux personnels, en accordant une attention particulière au problème de vie privée, d'âge, de lieu approprié, de harcèlement et de danger liés aux inconnus	Dès que les enfants commencent à utiliser Internet par eux-mêmes, discutez et établissez une liste de règles avec lesquelles vous êtes d'accord. Ces règles doivent inclure les horaires auxquels les enfants peuvent utiliser Internet et comment ils peuvent l'utiliser.
	4.	Définissez des règles pour un usage mobile	Dès que les enfants commencent à utiliser des téléphones mobiles, discutez et établissez une liste de règles avec lesquelles vous êtes d'accord. Ces règles doivent indiquer si les enfants ont la permission d'utiliser leur téléphones mobiles pour aller sur Internet et à quelle fréquence ils peuvent s'en servir, quel type de matériel ils peuvent acheter ou télécharger à l'aide des téléphones mobiles, comment gérer les choses inappropriées et le niveau de dépenses autorisé.

Parents, tuteurs et éducateurs			
	#	Domaines essentiels à considérer	Description
Education des parents, tuteurs et éducateurs	5.	Les parents doivent se familiariser avec les sites Internet utilisés par leurs enfants (i.e. services et produits proposés par les sites) et avoir une bonne compréhension de la manière dont les enfants passent leur temps en ligne	Evaluez les sites que vos enfants ont prévu d'utiliser et lisez soigneusement la politique de confidentialité, les conditions d'utilisation, le code de bonne conduite (souvent appelé «règlement intérieur»), ainsi que toute page dédiée aux parents. Cherchez également si le site surveille le contenu posté sur les pages de services et passe en revue périodiquement la page de votre enfant. Vérifiez si des produits sont vendus sur le site.
	6.	Etudiez les ressources en ligne pour trouver de plus amples informations concernant la sécurité sur Internet et la façon d'utiliser Internet de manière positive	L'usage positif et plus sûr d'Internet est célébré dans le monde entier tous les ans. Cela implique les enfants, les écoles locales, l'industrie et les acteurs pertinents collaborant afin de créer une plus grande conscience des opportunités de promouvoir une expérience en ligne positive. Pour trouver les informations les plus récentes sur ces événements, recherchez en ligne les termes «Internet sécurité célébration» + «nom du pays».
	7.	Comprenez comment les enfants utilisent d'autres terminaux personnels tels que les téléphones mobiles, les consoles de jeux, lecteurs de MP3 et PDA	Aujourd'hui, il est possible d'accéder à Internet par plusieurs types de terminaux personnels, donc les problèmes de sécurité peuvent également apparaître dans ces environnements.

	#	Domaines essentiels à considérer	Description
Revue des fonctionnalités des sites web	8.	Estimez si les programmes de filtrage et blocage ou ceux de contrôle peuvent servir d'appui ou de soutien aux enfants et jeunes afin qu'ils utilisent Internet et les équipements personnels de manière sûre. Si vous utilisez de tels logiciels, expliquer ce qu'ils font et pourquoi vous les utilisez avec vos enfants. Gardez secrets les mots de passe associés à ces programmes	Des questions de confiance et du droit d'un jeune à une vie privée peuvent émerger lorsque des outils techniques sont utilisés, en particulier les programmes de surveillance. Dans des circonstances normales il est nettement préférable qu'un parent ou un tuteur discute de ses raisons de vouloir utiliser ce type de logiciels, et dans les écoles leur utilisation doit également être expliquée.
	9.	Consentement parental	Certains pays, comme l'Espagne et les Etat-Unis, ont des lois spécifiant l'âge minimum auquel une entreprise ou un site web peut demander à un jeune de fournir des informations personnelles le concernant sans obtenir au préalable de consentement parental. Dans le cas de l'Espagne, cet âge est fixé à 14 ans, dans celui des Etat-Unis, il s'agit de 13 ans. Dans d'autres pays, il est considéré comme une bonne pratique d'exiger l'accord parental avant de demander aux jeunes de fournir de données personnelles. De nombreux sites accueillant les enfants les plus jeunes demandent l'accord parental avant de permettre aux enfants de s'inscrire. Vérifiez quelles sont les prescriptions en matière de consentement pour les sites auxquels vos enfants veulent s'inscrire ou dont ils sont membres.
	10.	Utilisation contrôlée des cartes et autres moyens de paiement	Surveillez l'usage de des téléphones mobiles ou fixes pour l'achat d'objets virtuels. La tentation peut être trop forte lorsqu'il est permis aux enfants d'utiliser des téléphones mobiles ou fixes pour acheter tous types de biens ou de services. Veillez également à garder en sécurité vos cartes bancaires, et à ne pas divulguer vos codes.
	11.	Assurez-vous que la vérification de l'âge est mise en place lors de l'achat de biens et de services en ligne	En général l'âge n'est pas vérifié lors de l'achat de marchandise, toutefois des systèmes deviennent accessibles pour garantir une vérification de l'âge au point de vente. Dans tous les cas, surveillez de près tous les achats en ligne de vos enfants.

	#	Domaines essentiels à considérer	Description
	12.	Vérifiez si le site Internet utilise une modération	Assurez-vous que le site Internet modère les conversations, idéalement à la fois à l'aide de filtres automatiques et d'une surveillance humaine. Est-ce que le site passe en revue toutes les photographies et vidéos qui y sont mises en ligne?
	13.	Bloquez l'accès aux contenus ou services indésirables	Les outils techniques peuvent vous aider à bloquer l'accès à des sites indésirables, par exemple ceux autorisant des contenus et discussions non-modérés, ou à bloquer l'accès à des services ou contenus sur téléphones mobiles.
	14.	Vérifiez la flexibilité contractuelle	Vérifiez comment supprimer un compte – même si cela signifie la perte de frais d'inscription. Si le service n'autorise pas la suppression d'un compte, envisagez de ne pas l'utiliser ou de bloquer son accès. Signalez cette impossibilité de suppression aux autorités locales.
	15.	Regardez le domaine d'application du service	Analysez les politiques des fournisseurs de contenus et leur conformité, vérifiez le contenu et les services spécifiques fournis et soyez conscients des limitations techniques (il est possible que les publicités ne soient pas clairement affichées comme telles).
	16.	Observez la publicité et signalez toute publicité inappropriée	Garder un œil sur les publicités et signalez à l'organisme chargé de vérifier les publicités toutes les publicités qui: 1. induisent en erreur en simplifiant à outrance des sujets compliqués 2. encouragent les enfants à parler à des inconnus, ou à aller dans des endroits dangereux 3. affichent des personnes, en particulier des enfants, utilisant des objets dangereux ou étant près de choses dangereuses 4. encouragent une émulation risquée ou des pratiques dangereuses 5. encouragent le harcèlement 6. causent aux enfants des préjudices moraux ou des peurs 7. encouragent de mauvaises pratiques alimentaires 8. exploitent la crédibilité des enfants.

W

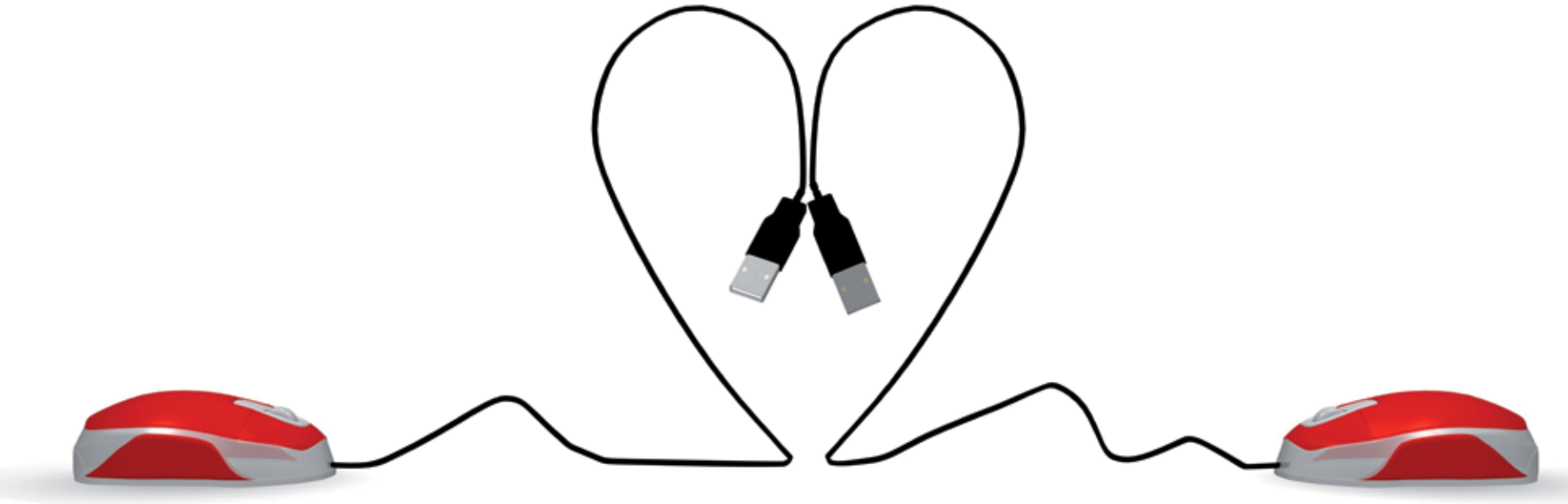
	#	Domaines essentiels à considérer	Description
Education des enfants	17.	Eduquez vos enfants	L'apprentissage et l'éducation aux média sont cruciaux. Expliquez les lignes directrices et les règles du monde virtuel. Les enfants vont probablement adhérer aux lignes directrices et souvent rappeler aux autres de faire de même. Apprenez à vos enfants à ne pas répondre à des messages impolis et à éviter les discussions concernant le sexe en ligne. Apprenez-leur à n'ouvrir aucune pièce jointe ou lien qu'ils recevraient lors d'une discussion, car ils peuvent contenir des données malfaisantes.
	18.	Expliquez à vos enfants de ne jamais organiser de rendez-vous réel avec une personne rencontrée pour la première fois en ligne	Les enfants peuvent être réellement en danger s'ils rencontrent en personne les étrangers avec lesquels ils ont communiqué en ligne. Les parents doivent encourager les enfants à n'utiliser les sites Internet que pour communiquer avec les amis hors ligne, et non avec des personnes qu'ils n'ont jamais rencontrées en personne. Les gens sur Internet peuvent ne pas être ceux qu'ils disent être. Toutefois si une forte amitié se lie en ligne et que votre enfant souhaite organiser une rencontre, plutôt que de le laisser se rendre seul ou sans escorte au rendez-vous, indiquez clairement que vous préférez être présent ou vous assurer qu'un autre adulte de confiance est présent, et assurez-vous que le premier rendez-vous ait lieu dans un lieu public bien éclairé et qu'il y a de nombreuses autres personnes autour.
	19.	Empêchez les enfants de partager des informations personnelles identifiables	Aidez vos enfants à comprendre quelles informations doivent rester confidentielles. Expliquez que les enfants ne doivent poster que des informations avec lesquelles vous – et ils – sont à l'aise et qu'ils veulent bien partager avec d'autres. Rappelez à vos enfants qu'une fois qu'ils ont posté des informations en ligne, ils ne peuvent plus les effacer.
	20.	Assurez-vous que les enfants comprennent ce que cela signifie de poster des photographies sur Internet, y compris à l'aide de webcams	Expliquez à vos enfants que les photographies peuvent révéler beaucoup d'informations personnelles. Il ne devrait pas être permis aux enfants d'utiliser des webcams ou de mettre en ligne de contenu sans l'accord d'un parent, d'un tuteur ou d'un adulte responsable. Encouragez vos enfants à ne pas poster de photographies d'eux-même ou de leurs amis avec des détails clairement identifiables tels que des plaques de rue, des plaques d'immatriculation sur des voitures, ou le nom de leur école sur leurs vêtements.
	21.	Avertissez les enfants du danger à exprimer ses émotions à des inconnus	Les enfants ne doivent pas communiquer avec des étrangers directement en ligne. Expliquez que ce qu'ils écrivent peut être lu par tout le monde ayant accès au site et que les prédateurs ou harceleurs cherchent souvent les enfants qui expriment un intérêt pour se faire de nouveaux amis en ligne.

	#	Domaines essentiels à considérer	Description
Revue de l'usage sûr des sites Internet	22.	Vérifiez la page ou le profil de votre enfant	Vérifiez de manière régulière la page de votre enfant. Connectez-vous pour visualiser l'historique du compte de votre enfant et si nécessaire modifiez le mode de discussion de votre enfant en un niveau avec lequel vous êtes à l'aise. Les sites Internet bien conçus vous offrent la possibilité de beaucoup vous impliquer dans l'expérience de votre enfant. Si votre enfant refuse de respecter les règles du site, vous pouvez envisager de contacter le site pour faire retirer la page et le profil de votre enfant. Cela peut entre autre renforcer votre message à votre enfant concernant l'importance de ces règles et les conséquences de les outrepasser.
	23.	Assurez-vous que les enfants correspondent aux limites d'âge du site Internet	Si les enfants sont d'âge inférieur à l'âge recommandé par les sites Internet, ne les laissez pas utiliser les sites. Il est important de se rappeler que les parents ne peuvent pas se reposer uniquement sur la capacité du fournisseur de service à éviter que les enfants trop jeunes ne s'enregistrent.
	24.	Assurez-vous que les enfants n'utilisent pas leur nom complet	Lorsque cela est possible, faites utiliser des surnoms à vos enfants – et non leur vrai nom ou des parties de leur nom. Les surnoms doivent être choisis soigneusement, pour ne pas attirer une attention inappropriée. Ne permettez pas à vos enfants de poster le nom complet de leurs amis ou toute autre information qui pourrait être utilisée pour les identifier, comme le nom de la rue où ils habitent, où ils vont à l'école, leur numéro de téléphone, leur club de sport, etc.
Communication	25.	Communiquez avec vos enfants à propos de leurs expériences	Parlez régulièrement avec vos enfants des sites qu'ils consultent et avec qui ils discutent en ligne. Encouragez vos enfants à vous raconter lorsqu'ils font face à quelque chose sur Internet qui les met mal à l'aise ou leur fait peur. Rappelez à vos enfants d'arrêter immédiatement quoiqu'ils soient en train de faire s'ils se sentent mal à l'aise ou ont des soupçons. Assurez-vous qu'ils comprennent qu'ils ne vont pas s'attirer d'ennuis s'ils vous signalent quelque chose. En échange, en tant parent et adulte, vous ne devez pas réagir de façon excessive lorsque votre enfant vous fait part de ses expériences. Restez calme quoiqu'ils vous racontent, rassemblez les faits, puis agissez. Félicitez votre enfant pour vous avoir fait confiance. Assurez-vous que les enfants puissent signaler les abuseurs.

Educateurs[52]			
		Domaine essentiel à considérer	**Description**
Sûreté et sécurité comme éléments des stratégies de protection des enfants	1.	Utilisez une approche impliquant tout l'établissement par rapport à la responsabilité de la sécurité en ligne	Il est important que même si les écoles n'autorisent pas l'utilisation de certains technologies au sein de l'école, elles apprennent aux élèves à se comporter raisonnablement et de manière appropriée lorsqu'ils les utilisent et qu'elles leur apprennent quels sont les risques.
	2.	Développer une politique d'utilisation acceptable (AUP)	Elle doit détailler de quelle manière le personnel, les élèves et tous les utilisateurs du réseau (y compris les parents) peuvent et ne peuvent pas utiliser les installations TIC.
Règles et politiques	3	Des exemples d'AUP sont disponibles à la fois en ligne et via les autorités locales.	Il est important d'adapter ces règles au contexte particulier de votre établissement.
	4	Liez les AUP aux autres politiques de l'école.	Cela doit inclure les politiques telles que celles concernant le harcèlement scolaire et les droits d'auteur et plagiat.
	5.	Point de contact unique	Désignez un membre haut placé de l'équipe de direction ayant la responsabilité de la sécurité pour qu'il soit également le point de contact central pour tous les problèmes de sécurité en ligne.
	6.	Besoin de direction	Les professeurs principaux, aidés des responsables, doivent prendre la direction pour faire passer à la pratique les politiques sur lesquelles il y a un consensus.
Être inclusif	7.	Maintenez la conscience parmi les jeunes	Assurez-vous que les jeunes dont vous avez la responsabilité sont conscients des risques potentiels et de la manière dont ils peuvent agir de façon sûre, avec un comportement responsable, qu'ils soient en ligne et où qu'ils le soient.
	8.	Soutenez la résilience	Permettez aux jeunes de développer leurs propres stratégies de protection pour les moments où la supervision d'un adulte ou la protection technologique ne sont pas possibles.

[52] BECTA (2008), *Safeguarding children online. A guide for school leaders* est disponible ici: www.becta.org.uk/schools/safety

		Domaines essentiels à considérer	Description
	9.	Encouragez la divulgation des méfaits et la prise de responsabilités	Aidez les jeunes à comprendre qu'ils sont responsables des actions que d'autres peuvent leur imposer, mais qu'il existe des sanctions que l'école appliquera s'ils n'agissent pas de manière appropriée lorsqu'ils sont en ligne.
Solutions techno-logiques	10.	Faites un audit des pratiques	Assurez-vous que les mesures et solutions technologiques sont régulièrement revues et mises à jour pour assurer une maintenance d'un programme efficace pour la sécurité en ligne.
Politiques de sécurité sur Internet	11.	Apprenez aux enseignants les politiques de sécurité sur Internet	Sensibilisez les enseignants à la sécurité sur Internet pour aider et soutenir les enfants à être en sécurité sur le Net.
	12.	Apprenez aux étudiants à ne jamais donner d'informations personnelles lorsqu'ils communiquent avec d'autres personnes	Informez les étudiants que les informations personnelles (par exemple: le nom complet, l'adresse, l'adresse électronique, le numéro de téléphone, l'école, etc.) ne doivent jamais être communiquées à des étrangers en ligne.
	13.	Exigez des étudiants qu'ils ne fassent que des recherches spécifiques	Exigez des étudiants qu'ils ne recherchent que des informations spécifiques, par opposition à «surfer» au hasard sur Internet et faites leur enregistrer, dans un format bibliographique, les URL des sites qu'ils ont consultés.
	14.	Prévisualisez ou testez les sites web avant d'envoyer des liens aux étudiants	Assurez-vous d'avoir visité personnellement tous les sites avant de les recommander aux étudiants. Il est également judicieux de mettre un marque page sur les sites web en avance de phase avant d'inviter les étudiants à visiter les URL.



5. Conclusions

Les technologies de l'information et de la communication – ou TIC – ont transformé le style de vie moderne. Elles nous ont fourni les communications en temps réel, sans frontières et un accès quasiment illimité aux informations et à une large gamme de services innovants.

En même temps, elles ont également créé de nouvelles opportunités d'exploitation et d'abus. Sans garde-fous appropriés, les enfants – parmi les plus gros utilisateurs d'Internet – courent le risque d'accéder à les images violentes, sexuelles et perturbantes.

Sans le dévouement approprié à créer un cyber environnement sûr, nous ne remplirons pas notre rôle auprès de nos enfants. Bien qu'il y ait une prise de conscience croissante des dangers liés à l'usage risqué des TIC, il reste encore beaucoup de travail à faire.

Il est donc crucial que les parents et les éducateurs soient capables de décider avec les enfants de ce qui est approprié et sûr pour eux, ainsi que le comportement responsable à adopter face aux TIC.

En travaillant ensemble, les parents, les éducateurs et les enfants peuvent récolter les bénéfices des TIC, en même temps qu'ils minimisent les dangers possibles pour les enfants.

Nous supposons que ces lignes directrices vont fournir des informations claires et compréhensibles concernant la protection des enfants en ligne, les risques auxquels les enfants peuvent faire face et ce que les parents et les éducateurs peuvent faire pour protéger et aider leurs enfants à comprendre comment tirer le meilleur parti des TIC tout en minimisant les dangers.

Sources et références à lire

En anglais:

Children's Online Privacy Protection Act (COPPA) http://www.coppa.org/coppa.htm

Cyberpeace Initiative, disponible ici: www.smwipm.cyberpeaceinitiative. org

Cyril. A. Wantland, Subhas C. Gupta, Scott A. Klein, Safety considerations for current and future VR applications, disponible ici: www.webmed.com/i-med/mi/safety.html (dernière visite le 4 septembre 2008).

'Are ads on children's social networking sites harmless child's play or virtual insanity?', The Independent, 2 juin 2008, disponible ici: www.independent.co.uk/news/media/are-ads-on-childrens-social-networking-sites-harmless-childs-play-or-virtual-insanity-837993.html (dernière visite le 11 juin 2008).

'Children's social-networking sites: set your little monsters loose online', Telegraph.co.uk, 17 novembre 2007, disponible ici: www.telegraph.co.uk/connected/main.jhtml?xml=/connected/2007/11/17/dlchildren17.xml (dernière visite le 10 juin 2008).

CBC News, Cyber-bullying, 2005, disponible ici: www.cbc.ca/news/background/bullying/cyber_bullying.html (dernière visite le 4 septembre 2008).

Child Exploitation and Online Protection Centre (CEOP): Think You Know, disponible ici: www.thinkuknow.co.uk/parents/gaming/bad.aspx (dernière visite le 4 septembre 2008).

Children, Adolescents, and Television, American Academy of Pediatrics, Pediatrics, Vol. 107, No. 2, février 2001, disponible ici: http://aappolicy.aappublications.org/cgi/content/full/pediatrics;107/2/423 (dernière visite le 10 septembre 2008).

Cyber-bullying: Developing policy to direct responses that are equitable and effective in addressing this special form of bullying, Canadian Journal of Educational Administration and Policy, Issue n. 57, 18 décembre 2006, disponible ici: www.umanitoba.ca/publications/cjeap/articles/brown_jackson_cassidy.html (dernière visite le 2 septembre 2008).

eModeration, Virtual World and MMOG Moderation: Five techniques for creating safer environments for children, May 2008, disponible ici: www.emoderation.com/news/press-release-virtual-world-and-mmog-whitepaper (dernière visite le 22 juillet 2008).

Entertainment & Leisure Software Publishers Association (ELSPA), Unlimited learning – Computer and video games in the learning landscape, disponible ici: www.elspa.com/assets/files/u/unlimitedlearningtheroleof-computerandvideogamesint_344.pdf (dernière visite le 26 août 2008).

ENISA, Children on virtual worlds – What parents should know, septembre 2008, disponible ici: www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf

Gauntlett, David and Lizzie Jackson, Virtual worlds – Users and producers, Case study: Adventure Rock, Communication and Media Research Institute (CAMRI), University of Westminster, UK, disponible ici: www.childreninvirtualworlds.org.uk/pdfs/gauntlett_and_jackson_may_2008.pdf

Home Office, Home Office Task Force on Child Protection on the Internet – Good practice guidelines for the providers of social networking and other user interactive services 2008, 2008, disponible ici: http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance?view=Binary (dernière visite le 16 juin 2008).

Home Office, Good practice guidance for the providers of social networking and other user interactive services 2008, disponible ici:

http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance (dernière visite le 12 septembre 2008).

Home Office, Good Practice Guidance for the Moderation of Interactive Services for Children, disponible ici: http://police.homeoffice.gov.uk/publications/operational-policing/moderation-document-final.pdf (dernière visite le 12 septembre 2008).

http://disney.go.com/fairies/pixiehollow/comingsoon.html (dernière visite le 26 août 2008).

www.redherring.com/Home/24182 (dernière visite le 10 juillet 2008).

Internet Watch Foundation: Protection Online www.iwf.org.uk/public/page.36.htm

Keith, Stuart, 'SpongeBob is the real threat to our children online', The Guardian, 10 avril, 2008, disponible ici: www.guardian.co.uk/technology/2008/apr/10/games.news (dernière visite le 10 juillet 2008).

Kirriemuir J., A Survey of the Use of Computer and Video Games in Classrooms, Nesta Futurelab Series, 2002, disponible ici: http://ccgi.goldingweb.plus.com/blog/wp-content/games_review1.pdf (dernière visite le 2 septembre 2008).

Kramer, Staci D., Disney Acquires Club Penguin; $350 Million Cash, Possible $350 Million Earnout, paidContent.org, 1 août 2007, disponible ici: www.paidcontent.org/entry/419-disney-acquires-club-penguin-in-deal-values-at-700-million-to-be-brande/ (dernière visite le 10 juillet 2008).

Mediashift, Virtual Worlds for Children Entwined with Real World, disponible ici: www.pbs.org/mediashift/2007/06/your_take_roundupvirtual_world.html (dernière visite le 28 août 2008).

Microsoft, How to help your children' use social networking Web sites more safely, 9 novembre 2006, disponible ici: www.microsoft.com/protect/family/activities/social.mspx (dernière visite le 11 juin 2008).

NSPCC: Children and the Internet www.nspcc.org.uk/whatwedo/mediacentre/mediabriefings/policy/children_and_the_internet_media_briefing_wda49338.html

The Children's Charity: Net Smart Rules www.nch.org.uk/information/index.php?i=135

Virtual Worlds Management, Disney.com Launches Games and Virtual Worlds Portal; Mobile Widgets, 14 août 2008, disponible ici: www.virtualworldsnews.com/2008/08/disneycom-launc.html (dernière visite le 26 août 2008).

Virtual Worlds Management, Virtual Worlds Managements Youth Worlds Analysis, 22 août 2008, disponible ici: www.virtualworldsmanagement.com/2008/youthworlds0808.html (dernière visite le 25 août 2008).

Virtual Worlds News, Virtual World 125,000 Children Fight Obesity in Whyville, disponible ici: www.virtualworldsnews.com/2007/06/virtual_world_h.htm (dernière visite le 4 septembre 2008).

Programmes ambassadeurs pour la formation des formateurs – divers sites en sont de bons exemples. www.thinkuknow.co.uk/teachers/training.aspx www.saferinternet.at/tipps/fuer-eltern/

Matériel d'éducation. Il existe d'excellentes ressources disponibles pour délivrer des messages de sécurité en ligne. La liste suivante n'est pas exhaustive, d'autres ressources sont consultables ici www.saferinternet.org/ww/en/pub/insafe/resources.cfm.

www.digizen.org/cyberbullying/film.aspx – est une excellente ressource utilisée par plusieurs sites pour combattre le harcèlement.

www.internetsanscrainte.fr/le-coin-des-juniors/dessin-anime-du-mois – Vinz et Lou – des dessins animés français dont l'objectif est de faire prendre conscience des problèmes de sécurité en ligne.

www.cyberethics.info/cyethics2/page.php?pageID=25&mpath=/35 – fournit un ensemble de bonnes astuces pour les enseignants.

http://www.easy4.it/content/category/13/59/104/ – matériels issus du site Italien destiné à soutenir les enseignants.

www.teachtoday.eu/en/Lesson-Plans.aspx – ce site fournit un ensemble de plans de cours conçus pour être utilisés dans les écoles. Le site est en cours de mise à jour et plus d'informations seront bientôt disponibles.

http://dechica.com – un jeu permettant aux jeunes enfants de prendre

conscience, développé par le nœud bulgare.

www.microsoft.com/cze/athome/bezpecnyinternet – version flash de la brochure divertissante sur la manière dont on peut utiliser Internet plus sûrement édité par Microsoft. Promotion faite au cours de la journée *Safer Internet Day 2009*.

www.tietoturvakoulu.fi – usage sûr d'Internet et test «Soyez malin sur le Web».

Entretiens vidéo avec des célébrités lettones qui expriment leur opinion et leur expérience personnelle concernant le harcèlement en ligne. Langue(s): letton.

Plus d'entretiens:
Vidéo 2 (célébrité TV): www.youtube.com/watch?v=QttMrRABnR0&feature=related

Vidéo 3 (danseur): www.youtube.com/watch?v=3cPRlhQDJAg&feature=related

Vidéo 4 (pilote de rally): www.youtube.com/watch?v=PodsmBjrE6Y&feature=related

Vidéo 5 (politicien): www.youtube.com/watch?v=4_xrUvDQaIY&feature=related

Vidéo 6 (chanteur): www.youtube.com/watch?v=usqpmAHjHQ4

www.tietoturvakoulu.fi. – les parents peuvent tester leurs connaissances de l'éducation média avec ce test en ligne sur le site web. Langues: finnois et suédois.

www.medieradet.se/bestall--ladda-ner/filmrummet – une partie du site web du Conseil des médias suédois est dédiée à du matériel image émouvant. Langue(s): suédois et parties en anglais.

www.lse.ac.uk/collections/EUKidsOnline/ – recherche européenne sur les questions culturelles et contextuelles, ainsi que les risques relatifs a à l'utilisations sûre d'Internet et des nouveaux médias par les enfants.

http://www.nortononlineliving.com/ fournit un instantané des tendances dans plusieurs pays.

www.pewinternet.org/ – Pew fournit un grand ensemble de rapports concernant l'utilisation d'Internet et des technologies en relation. Bien que basé aux USA, l'historique a montré que les tendances qui commencent aux USA tendent à migrer vers l'UE au fil du temps.

www.unh.edu/ccrc/ – recherche de David Finkelhor concernant les tendances en termes d'arrestations de prédateurs sur Internet qui suggèrent qu'il n'y a pas de preuve réelle pour soutenir l'assertion selon laquelle Internet a créé plus de prédateurs.

www.webwise.ie/article.aspx?id=10611 – recherche menée par le nœud irlandais.

www.childnet-int.org/youngpeople/

www.kidsmart.org.uk

www.chatdanger.com

Appendice 1

La protection intégrée

Les PC et les Mac ont des contrôles parentaux intégrés dans leur système d'exploitation, et chacun de leur nouveaux systèmes (Windows Vista et Leopard de Mac). Si vous envisagez de mettre à jour votre système d'exploitation, cela peut vous épargner le coût d'un logiciel de surveillance supplémentaire.

Afin d'utiliser les contrôles de votre ordinateur, veuillez d'abord créer des comptes utilisateurs individuels pour chacun de vos enfants. Vérifiez le guide utilisateur de votre ordinateur si vous n'êtes pas certain de la façon dont vous devez procéder.

Utilisateurs de Mac: Ensuite, choisissez Préférences Système dans le menu Apple, et cliquez sur Comptes. Pour chacun des comptes des enfants, cliquez sur Contrôle parental et il vous sera proposé une liste de catégories (Mail, Safari, etc.) que vous pouvez restreindre ou surveiller.

Si vous fonctionnez sous Leopard, vous pouvez enregistrer les conversations IM et indiquer à qui votre enfant peut parler via courrier électronique ou iChat, entre autre. Vous pouvez également limiter le temps d'écran. Par exemple, vous pouvez configurez votre ordinateur pour qu'il déconnecte automatiquement vos enfants à 20h.

Utilisateurs Windows: Les contrôles parentaux sont accessibles via le Panneau de contrôle. Cherchez Comptes utilisateurs et Panneau de contrôle Sécurité familiale. Avec Windows Vista, vous aurez le choix concernant des restrictions web et également l'option de recevoir des rapports sur l'utilisation de votre enfant de l'ordinateur. Vous pouvez indiquer certaines heures hors-limites et bloquer les jeux vidéo et programmes répréhensibles.

Peu importe le système que vous ayez, la plupart des navigateurs (Safari, Firefox, etc.) ont un journal de l'historique automatique qui indique quels sites ont été consultés. Consultez le manuel utilisateur pour apprendre comment vérifier l'historique, si vous n'êtes pas familier avec la procédure. Assurez-vous de vérifier tous les navigateurs de votre ordinateur si vous en avez plus d'un. Et soyez averti: les enfants peuvent apprendre comment effacer l'historique pour couvrir leurs traces, donc posez des questions si vous vous rendez compte que l'historique a été effacé par quelqu'un d'autre que vous.

Vous avez besoin d'aide? A la fois Apple (Mac) et Microsoft (Windows) ont des tutoriaux en ligne et des informations détaillées sur leur sites web – tapez simplement «contrôle parental» et «Apple» ou «Microsoft» dans Google pour les trouver.

Gardez à l'esprit que toute protection que vous essayez de fournir à vos enfants sera, bien sûr, incomplète. Vous devez communiquer avec vos enfants autant que possible et discuter avec eux des problèmes de protection des enfants en ligne.

Appendice 2

Le langage instantané décodé

Les abréviations et mots de code accélèrent les discussions par messagerie instantanée et par service de messagerie SMS, mais peuvent également masquer ce que les personnes disent! Préparez-vous. Voici quelques termes fréquemment utilisés:

En anglais:

ADIH: Another day in hell / un autre jour en enfer

A/S/L: Age, sex, location / âge, sexe, ville

BTDT: Been there done that / j'y étais, je l'ai fait

CULTR: See you later / à plus tard

GTFO: Get the f-ck out (exprime la surprise)

H8: Hate / déteste

ILY or 143 or <3: I love you / je t'aime

JK or J/K: Just kidding / je plaisante

KWIM: Know what I mean? / tu vois ce que je veux dire?

LLS: Laughing like sh-t / mort de rire

LMIRL: Let's meet in real life / rencontrons-nous dans la vraie vie

LYLAS (B): Love you like a sister (brother) / je t'aime comme une soeur (un frère)

NIFOC: naked in front of computer / nu devant l'ordinateur

PAW or PIR or P911: Parents are watching or parent in room / les parents surveillent ou les parents sont dans la pièce (changes de sujet)

POS: Parent over shoulder / les parents lisent par dessus mon épaule (peut également signifier «piece of sh-t» (espèce de merde) utilisé comme insulte)

Pr0n: faute d'orthographe intentionnelle de «porn»

STFU: Shut the f-ck up / la ferme (exprime la surprise plutôt qu'une réprimande)

TMI: Too much information / trop d'informations

TTFN: Ta ta, for now / c'est tout pour l'instant (au revoir)

WTF: What the f-ck? / qu'est-ce que c'est que ça?

Source: http://www.parenting.com/article/Mom/Relationships/How-to-Spy-on-Your-Child-Online/3

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

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

Imprimé en Suisse
Genève, 2011

Avec la participation et le soutien de:

CHIS

THE UNIVERSITY OF EDINBURGH

ins@fe

CYBER Peace Initiative

enisa European Network and Information Security Agency