

# Atelier sur le contrôle parental

Vos enfants connaissent Internet mieux que vous!

Dans le cadre de cet atelier de contrôle parental, il a été décidé d'élaborer une liste d'informations pour des parents soucieux de la sécurité de leurs enfants. Dans le but de préserver notre accès à Internet, il est de notre devoir de mettre en œuvre les moyens nécessaires pour contrôler nos enfants au lieu de leur interdire l'accès à certain site Web et de les éduqués à la bonne utilisation de cette ressource.

Sur Internet, le meilleur côtoie le pire. La question de la responsabilité des contenus qui circulent sur la Toile reste encore sans réponse satisfaisante. Est-ce que ce sont les fournisseurs d'hébergement ou d'accès Internet ? Tant que le législateur n'aura pas clairement défini les responsabilités de chacun, c'est à l'internaute de se responsabiliser.

*[- Vidéo -] ~ 35min*

*[- Discussion -] ~ 15min*

## Atelier d'information

L'enfant est exposé aux contenus inappropriés de manière différente suivant le type de données accessibles et l'outil qu'il utilise pour y accéder. L'âge influence aussi quel type de recherche ils feront à partir des connaissances qu'ils ont obtenues d'amis ou encore de la télévision.

### **Risque d'Internet pour vos enfants**

- Se retrouver sur des sites, à caractère pornographe, pédophile ou prônant le racisme, le recours à la violence et au terrorisme !
- Avoir accès à des informations dangereuses (fabrication de bombes, de fusée, de poison, etc.)

- Echanger sans méfiance avec des inconnus, qui peuvent à la fois tenter de les attirer, de les manipuler, et obtenir d'eux des informations confidentielles concernant votre famille.
- Participer à différentes chaînes ou trafics : stupéfiants, logiciels.
- Pirater par défi, goût du risque ou intérêt, et se lancer dans la contrefaçon !
- Laisser inoculer, par ignorance, votre ordinateur par des virus ou pire : des « chevaux de Troie » permettant la divulgation de tout ce que contient le disque dur.
- L'enfermement dans un monde virtuel, les coupant de la réalité, et pouvant aboutir à la dépression, et quelquefois au suicide !

## **Risque d'Internet pour vous**

- Retrouver vos données confidentielles divulguées et utilisées avec des intentions souvent malveillantes, votre compte débité à votre insu !
- Permettre le cambriolage de vos biens, facilité par les renseignements sur vos habitudes, obtenus de vos enfants sur des forums !
- Voir votre ordinateur inoculé par des virus, ou « chevaux de Troie » et perdre vos données.
- Voir votre enfant s'isoler et perdre le contact avec la réalité et avec vous.
- Voir votre enfant se lancer dans des expérimentations dangereuses pour lui !
- Devoir répondre devant les tribunaux des erreurs et des infractions de vos enfants.

## **Conseils de sécurité par âge (2 à 4 ans)**

Une étude réalisée en 2003 a révélé que les enfants du préscolaire représentent un des groupes d'utilisateurs d'Internet les plus en croissance. Bien que les 2 à 4 ans aient une capacité de concentration trop courte pour faire des activités en ligne, les images et les sons peuvent stimuler leur imagination et s'intégrer à leurs premières expériences du monde qui les entoure.

Parents, frères et sœurs plus âgés les initient à Internet, leur font découvrir des sites et des jeux. La tâche principale des adultes est de commencer à leur enseigner les principes de la sécurité sur Internet et de surveiller de près leurs réactions aux différents contenus qu'ils découvrent.

## Conseils de sécurité

- Ne laissez jamais des enfants de cet âge seuls en ligne.
- Personnalisez leur environnement Internet en créant une liste de « favoris » que vous aurez choisis.
- Utilisez des moteurs de recherche pour enfants ou ceux offrant un contrôle parental.
- Considérez les filtres Internet comme un complément de sécurité qui ne remplace en aucun cas la supervision parentale.
- Protégez les 2 à 4 ans de l'apparition de publicités offensantes à l'aide d'un logiciel de blocage ou en désactivant Java.
- Commencez à leur apprendre à protéger leur vie privée. Si on demande leur nom pour « personnaliser » leur accès à un site, demandez-leur de choisir un surnom.
- Tous les membres de la famille devraient leur servir de modèles dans leur utilisation d'Internet.

## Les 2 à 4 ans :

- prennent les contenus en ligne au pied de la lettre ;
- n'ont pas le sens critique nécessaire pour naviguer seuls ;
- peuvent être effrayés par des images médiatiques, réelles ou fictives ;
- risquent d'être effrayés par une présentation réaliste de menaces, violences et dangers divers ;
- risquent de tomber sur des sites inappropriés en s'amusant à cliquer sur des liens.

## Conseils de sécurité par âge (5 à 7 ans)

Les 5 à 7 ans ont une vision positive du monde et sont encore très crédules. Ils sont fiers de commencer à savoir lire et compter, et ils adorent discuter et partager leurs idées. Ils acceptent facilement l'autorité, désirent bien se conduire et font confiance aux adultes.

Les enfants de cet âge sont déjà capables de se servir d'un ordinateur, qu'il s'agisse de suivre des consignes, manipuler la souris ou jouer à des jeux vidéo, mais ils ont encore besoin des adultes ou d'enfants plus âgés qu'eux pour trouver des sites Web, comprendre l'information en ligne ou envoyer un courriel.

## Conseils de sécurité

- Ne laissez jamais des enfants de cet âge seuls en ligne.
- Personnalisez leur environnement Internet en créant une liste de « favoris » qu'ils ont choisis avec vous.
- Utilisez des moteurs de recherche pour enfants ou ceux offrant un contrôle parental.
- Installez l'ordinateur dans un endroit passant de la maison afin de pouvoir superviser facilement leurs activités en ligne.
- Considérez les filtres Internet comme un complément de sécurité qui ne remplace en aucun cas la supervision parentale.
- Commencez à leur apprendre à protéger leur vie privée. Dites-leur de ne jamais donner en ligne d'informations les concernant, eux ou leur famille.
- Si on les encourage à donner leur nom pour « personnaliser » leur accès à un site, demandez-leur d'employer un surnom.
- Protégez-les de l'apparition de publicités offensantes à l'aide d'un logiciel de blocage ou en désactivant Java.
- À cet âge, vous devriez leur interdire l'accès aux messageries instantanées, courriels, bavardoirs ou babillards électroniques.
- Encouragez-les à venir vous voir si quelque chose sur Internet les effraie ou les met mal à l'aise. (Restez calme. Ne vous énervez

## Les 5 à 7 ans :

- prennent les contenus en ligne au pied de la lettre ;
- n'ont pas le sens critique nécessaire pour naviguer seuls ;
- peuvent être effrayés par des images médiatiques, réelles ou fictives ;
- risquent d'être effrayés par une présentation réaliste de menaces, violences et dangers divers ;
- sont une proie facile pour les publicitaires qui les encouragent à donner des informations personnelles en ligne par le biais de sondages, concours ou formulaires d'inscription ;
- risquent de tomber sur des sites inappropriés en s'amusant à cliquer sur des liens ;
- peuvent tomber sur des sites inappropriés lors d'une recherche en ligne.

pas, sinon ils n'oseront rien vous dire la prochaine fois qu'ils auront besoin de vous.)

## Conseils de sécurité par âge (8 à 10 ans)

La famille occupe encore une place très importante dans la vie des 8 à 10 ans. Ils s'intéressent également aux activités des enfants plus âgés qu'eux, commencent à affirmer leur propre personnalité, se montrent généralement confiants et ne remettent pas en question l'autorité des adultes.

Naviguer pour le plaisir et jouer à des jeux interactifs sont leurs activités favorites en ligne. Ils commencent à se servir du courriel et à utiliser aussi, parfois, les messageries instantanées, les bavardoirs et les babillards électroniques.

### Conseils de sécurité

- Établissez avec eux une liste de règlements à respecter sur Internet.
- Restez près d'eux quand ils naviguent sur Internet ou assurez-vous qu'ils ne visitent que les sites que vous avez autorisés.
- Gardez les ordinateurs branchés sur Internet dans un endroit passant de la maison que vous pouvez aisément surveiller.
- Considérez les filtres comme un complément de surveillance, mais qui ne peut pas remplacer votre supervision.
- Utilisez des moteurs de recherche conçus pour les enfants ou d'autres dotés de contrôles parentaux.
- Procurez-vous un compte de courriel familial auprès de votre

### Les 8 à 10 ans :

- sont curieux et avides de découvrir de nouvelles choses ;
- n'ont pas assez de sens critique pour naviguer seuls en ligne ;
- sont des proies faciles pour les sites commerciaux qui les encouragent à fournir des renseignements personnels dans les sondages, concours et formulaires d'inscription ;
- peuvent être effrayés par des représentations réalistes de situations violentes, menaçantes ou dangereuses ;
- commencent à communiquer en ligne avec des « amis » qu'ils

fournisseur de services Internet. Les 8 à 10 ans sont trop jeunes pour avoir leur propre compte.

- Apprenez à vos enfants à ne jamais donner de renseignements personnels en ligne sans votre autorisation, que ce soit par le biais des courriels, bavardoirs, babillards électroniques ou formulaires d'inscription, concours et profils personnels de sites Web.
- Servez-vous des filtres des courriels pour bloquer les messages non sollicités ou contenant certaines expressions ou mots inappropriés.
- Ne permettez pas aux jeunes de cet âge d'avoir accès aux messageries instantanées.
- Ne les laissez fréquenter que des bavardoirs et des babillards électroniques supervisés dans de bons sites pour enfants.
- Discutez avec eux de leurs amis et de leurs activités en ligne comme vous le faites pour toute autre chose dans le quotidien.
- Discutez avec eux de la sexualité et de l'importance de développer une attitude respectueuse et saine. Il est fort probable qu'ils tombent un jour par hasard sur des sites pornographiques.
- Encouragez-les à venir vous voir si quelque chose sur Internet les effraie ou les met mal à l'aise. (Restez calme. Si vous vous emportez, ils n'oseront rien vous dire la prochaine fois qu'ils auront besoin de vous.)

n'ont jamais rencontrés en personne ;

- peuvent être influencés par des images ou des personnalités médiatiques, en particulier celles qu'ils trouvent « cool » ou séduisantes ;
- peuvent tomber par hasard durant une recherche sur des sites Web inappropriés ;
- risquent d'être ciblés par des prédateurs dans les bavardoirs, babillards électroniques et messageries instantanées.

## Conseils de sécurité par âge (11 à 13 ans)

Le passage de la préadolescence à l'adolescence est une période de changements rapides dans la vie des jeunes. Ils ont encore besoin de leurs parents, mais veulent plus d'indépendance, accordent plus d'importance aux relations avec leurs amis et s'intéressent davantage aux réalités sociales qui les entourent.

C'est aussi le moment où ils se mettent à utiliser Internet non seulement pour leurs travaux scolaires, mais aussi pour télécharger de la musique, se servir du courriel, jouer à des jeux vidéo en ligne et voter pour leurs vedettes préférées sur les sites Web consacrés aux artistes. La messagerie instantanée devient le moyen de communication favori pour échanger avec leurs amis.

<b>Conseils de sécurité</b>	<b>Les jeunes de 11 à 13 ans :</b>
<ul style="list-style-type: none"><li>▪ Établissez avec eux une liste de règles d'utilisation d'Internet.</li><li>▪ Installez les ordinateurs branchés sur Internet dans des endroits passants de la maison, jamais dans leur chambre.</li><li>▪ Discutez de leurs amis et de leurs activités en ligne exactement comme vous le feriez dans la vie de tous les jours.</li><li>▪ Insistez auprès d'eux pour qu'ils vous préviennent avant de rencontrer en personne des « amis » qu'ils se sont faits en ligne.</li><li>▪ Apprenez-leur à ne jamais divulguer sans votre autorisation des renseignements personnels dans les courriels, bavardoirs, messageries instantanées,</li></ul>	<ul style="list-style-type: none"><li>▪ maîtrisent facilement les nouvelles technologies ;</li><li>▪ s'intéressent aux sous cultures étrangères à l'univers de leurs parents ;</li><li>▪ n'ont pas le sens critique nécessaire pour juger de l'exactitude d'une information trouvée en ligne ;</li><li>▪ acceptent sans discernement toutes les formes de jeux et de divertissement ;</li><li>▪ sont des proies faciles pour les stratèges du marketing qui les encouragent à fournir des renseignements personnels par le biais de sondages, concours ou formulaires d'inscription ;</li><li>▪ sont à un point sensible de leur développement sexuel ; les garçons, en</li></ul>

<p>formulaire d'inscription, profils personnels et concours de sites Web.</p> <ul style="list-style-type: none"><li>▪ Encouragez-les à venir vous voir si des messages ou des contenus les mettent mal à l'aise ou leur font peur. (Gardez votre calme. Si vous vous énervez, ils ne vous en parleront pas la prochaine fois.)</li><li>▪ Abordez avec eux le problème de la pornographie et orientez-les vers de bons sites sur la santé et la sexualité.</li><li>▪ Insistez pour avoir accès à leurs courriels et messageries instantanées pour vous assurer qu'ils n'y parlent pas à des inconnus.</li><li>▪ Enseignez-leur une attitude responsable en ligne. Ils peuvent enfreindre la loi du droit d'auteur par le biais des partages de fichiers ou en copiant des textes, photos ou illustrations trouvés sur un autre site Web.</li></ul> <ul style="list-style-type: none"><li>• Discutez également avec eux de la nécessité d'une conduite éthique. Ils ne devraient jamais se servir d'Internet pour répandre des rumeurs, harceler ou menacer les autres.</li><li>• Ne les laissez utiliser que des bavardoirs supervisés sur de bons sites pour enfants.</li><li>• Aidez-les à se protéger des pourriels. Dites-leur de ne pas donner leur adresse de courriel en ligne et de ne</li></ul>	<p>particulier, sont parfois tentés de visiter des sites pornographiques ;</p> <ul style="list-style-type: none"><li>▪ peuvent avoir envie (particulièrement les filles) de se lier d'amitié avec des inconnus rencontrés en ligne ;</li><li>▪ peuvent être harcelés ou harceler les autres en ligne.</li></ul>
---	---



<p>jamais répondre à un pourriel.</p> <ul style="list-style-type: none"> <li>• Servez-vous des filtres des courriels pour bloquer les messages en provenance de certaines personnes ou contenant certains mots ou phrases spécifiques.</li> </ul>	
---	--

## Conseils de sécurité par âge (14 à 17 ans)

Au début de l'adolescence, les jeunes peuvent passer par une période de manque de confiance en eux-mêmes et ont besoin de l'approbation de leurs pairs. Ils répondent moins aux attentes de leurs parents. Plus tard, les ados ont besoin d'indépendance et de s'identifier à un groupe, et commencent à établir un équilibre entre les valeurs de leurs parents et celles des jeunes de leur âge. À la fin de l'adolescence, ils sont plus mûrs et prêts à interagir à un niveau plus intellectuel avec le monde qui les entoure. La plupart des adolescents sont ouverts aux idées nouvelles, mais n'ont pas encore une expérience suffisante de la vie pour juger de leur validité.

Les adolescents téléchargent de la musique, utilisent courriels et messageries instantanées pour communiquer entre eux et se passionnent pour les jeux vidéo. Ils font aussi régulièrement usage des moteurs de recherche pour trouver de l'information sur Internet. La plupart des jeunes fréquentent des bavardoirs et s'aventurent parfois dans les salles privées ou les bavardoirs pour adultes. À cet âge, ils sont plus susceptibles de briser les interdictions et de visiter des sites présentant des blagues grossières, des scènes sanglantes, des jeux de hasard ou de la pornographie.

<p><b>Conseils de sécurité</b></p> <ul style="list-style-type: none"> <li>▪ Établissez avec eux une liste de règles d'utilisation d'Internet, qui devrait spécifier quel genre de sites leur est interdit.</li> <li>▪ Installez les ordinateurs branchés sur Internet dans des endroits passants de la maison,</li> </ul>	<p><b>Les jeunes de 14 à 17 ans :</b></p> <ul style="list-style-type: none"> <li>▪ manifestent davantage de sens critique et de discernement dans leurs intérêts et activités en ligne ;</li> <li>▪ sont plus susceptibles de recevoir en ligne des</li> </ul>
---	--

jamais dans leur chambre.

- Discutez de leurs amis et de leurs activités en ligne exactement comme vous le feriez pour toutes autres activités quotidiennes.
- Sachez quels bavardoirs et babillards électroniques ils fréquentent et à qui ils parlent. Encouragez-les à s'en tenir à des bavardoirs supervisés.
- Discutez avec eux de leur liste de messagerie instantanée et assurez-vous qu'ils ne parlent pas à des inconnus.
- Insistez auprès d'eux pour qu'ils vous préviennent avant de rencontrer en personne des « amis » qu'ils se sont faits en ligne.
- Apprenez-leur à ne jamais divulguer sans votre autorisation des renseignements personnels dans les courriels, bavardoirs, messageries instantanées, formulaires d'inscription, profils personnels et concours de sites Web.
- Encouragez-les à venir vous voir si des messages ou des contenus les mettent mal à l'aise ou leur font peur. (Gardez votre calme. Ne vous énervez pas, sinon ils ne vous diront rien la prochaine fois qu'ils auront besoin de vous.)
- Abordez avec eux la question de la pornographie en ligne et orientez-les vers de bons sites sur la santé et la sexualité.
- Insistez pour qu'ils restent toujours dans les salles

commentaires non sollicités à caractère sexuel ;

- reçoivent le plus grand pourcentage de pourriels pornographiques ;
- désirent souvent (particulièrement les filles) se lier d'amitié avec des inconnus rencontrés en ligne ;
- sont plus susceptibles de se faire demander un rendez-vous en personne et risquent davantage de l'accepter ;
- sont encore vulnérables aux stratégies de marketing qui les encouragent à fournir des renseignements personnels par le biais de sondages, concours ou formulaires d'inscription ;
- peuvent être tentés (les garçons en particulier) de visiter des sites pornographiques ;
- peuvent être harcelés ou harceler les autres en ligne ;
- sont plus susceptibles d'utiliser des cartes de crédit en ligne ;
- peuvent commencer à fréquenter des sites de paris ou jeux de hasard

<p>publiques des bavardoirs.</p> <ul style="list-style-type: none"><li>▪ Aidez-les à se protéger des pourriels. Dites-leur de ne pas donner en ligne leur adresse de courriel, de ne jamais répondre à un pourriel et d'utiliser les filtres des courriels.</li><li>▪ Tenez-vous au courant des sites Web qu'ils fréquentent et assurez-vous qu'on n'y trouve ni contenus offensants, ni photos et informations personnelles.</li><li>▪ Parlez-leur de l'importance d'adopter une attitude responsable en ligne. Ils peuvent enfreindre la loi du droit d'auteur par le biais des partages de fichiers ou en copiant photos, illustrations ou textes trouvés sur un autre site Web.</li><li>▪ Discutez également avec eux de la nécessité d'une conduite éthique. Ils ne devraient jamais se servir d'Internet pour répandre des rumeurs, harceler ou menacer les autres.</li><li>▪ Exigez de vos adolescents qu'ils vous préviennent avant toute transaction financière en ligne, commande, vente ou achat.</li><li>▪ Discutez avec eux des jeux de hasard, des risques qu'ils comportent, et rappelez-leur que la loi interdit aux mineurs de parier de l'argent en ligne.</li></ul>	
--	--

## Atelier Pratique

Pour bloquer l'accès aux contenus inadaptés, les logiciels de contrôle parental utilisent deux méthodes principales : le filtrage par

liste d'URL et le filtrage par mot clés. Le filtrage par liste est la méthode la plus répandue : la plupart des logiciels fonctionnent avec une base de données de sites déconseillés. Appelées aussi "listes noires", ces bases contiennent des adresses de sites classés selon les thèmes : il existe des dizaines de catégories comme le sexe, la violence, les armes, la religion ou la politique. Les parents peuvent choisir d'interdire une ou plusieurs catégories. Quand l'enfant veut visiter une page Web, l'URL du site est d'abord comparée à la liste noire du logiciel. Si l'adresse en question fait partie des sites déconseillés, l'enfant ne peut pas y accéder. Les logiciels qui pratiquent ce type de filtrage fonctionnent comme les anti-virus : pour être efficaces, ces listes doivent être régulièrement mises à jour.

**Attention :** la vitesse d'apparition de nouveaux sites rend impossible le recensement de toutes les adresses déconseillées. Pour résoudre ce problème, les éditeurs ont mis en place une méthode complémentaire : le filtrage par mot clé. Le logiciel définit à l'avance les mots non adaptés aux enfants et bloque tous les sites qui les contiennent. La plupart des logiciels donnent aussi la possibilité aux parents de constituer leurs propres listes des interdits. Exemple : si vous ne souhaitez pas que votre enfant passe son temps sur les sites de jeux vidéo trop violents pour son âge, vous pouvez interdire les mots relatifs à ce sujet.

Tout d'abord, avant de faire quelque installation que se soit, il est conseillé de faire les mises à jours de votre système d'exploitation. Il est bien entendu qu'il faut faire la même chose avec le logiciel anti-virus ou toute autre programme de protection de votre ordinateur. C'est mise a jours doive être fait régulièrement (une fois semaine minimum).



### **Internet Explorer**

Au sein de votre navigateur Internet Explorer, version 6, un gestionnaire d'accès vous aide à contrôler les types de contenu auxquels votre ordinateur peut accéder sur Internet. Une fois le gestionnaire d'accès activé, seul le contenu dont le contrôle d'accès correspond à vos critères peut être affiché. Vous pouvez moduler les paramètres.

Le gestionnaire d'accès vous permet de :

- Contrôler l'accès aux paramètres du Gestionnaire d'accès. Vous activez le Gestionnaire d'accès et en affichez les paramètres à l'aide d'un mot de passe. Vous avez besoin de ce mot de passe pour modifier les paramètres du Gestionnaire d'accès ; vous pouvez éventuellement le noter pour vous en souvenir ultérieurement.

- Afficher et définir les paramètres de contrôle d'accès en fonction du type de contenu que vous considérez comme acceptable dans chacune des quatre catégories suivantes : langue, nudité, sexe et violence.
- Définir les types de contenu que les autres utilisateurs peuvent afficher avec ou sans votre autorisation. Vous pouvez définir des exceptions individuelles aux paramètres de contenu.
- Définir la liste des sites Web dont l'accès est toujours interdit, indépendamment du contrôle d'accès de leur contenu.
- Définir la liste des sites Web dont l'accès est toujours autorisé, indépendamment du contrôle d'accès de leur contenu.

Afficher et modifier les systèmes de contrôle et de bureaux d'accès que vous utilisez. Lorsque vous l'activez pour la première fois, les paramètres par défaut du gestionnaire d'accès sont définis avec leurs valeurs les plus strictes (les moins susceptibles de choquer). Vous pouvez modifier ces paramètres en fonction de vos préférences personnelles.

Pour plus d'informations, consultez l'aide de votre navigateur sous l'onglet "?" et choisissez la rubrique "Gestionnaire d'accès".



### **Netscape**

Il n'existe aucun mode de filtrage des pages Web qui s'affichent dans ce navigateur dont nous avons installé la version 7.02.

Il y a néanmoins une possibilité de gérer les messages électroniques entrants au moyen de règles de filtrage et surtout, il y a un système de blocage des "popup" qui y est intégré.



### **Mozilla**

Nous n'avons pas constaté la présence d'une fonction de contrôle parental dans ce navigateur. Il existe néanmoins un système de filtrage de "Spam" pour ce qui est du module de messagerie électronique.



### **Opera**

Nous n'avons pas trouvé de fonctions de filtrage des sites Web dans la version 7.10 de ce navigateur. Il existe néanmoins un mode de tri intégré dans la messagerie électronique basé sur un système de règles de filtrage.

**Conseil :** Lorsque votre jeune s'inscrit à l'aide de formulaire, il serait bon qu'il utilise une adresse de messagerie fictive et non celle qu'il utilise habituellement. Des service de messagerie gratuit son disponible, par exemple Hotmail, Yahoo, Caramail, etc.