

Atelier sur le contrôle parental

Vos enfants connaissent Internet mieux que vous!

Dans le but de préserver notre accès à Internet, il est de notre devoir de mettre en œuvre les moyens nécessaires pour interdire à nos enfants l'accès à certains sites Web et de les éduquer à la bonne utilisation de cette ressource.

- Que faut-il filtrer?

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.

1) Cas des navigateurs

Les navigateurs les plus connus sont : Internet Explorer et Netscape.

Il est très facile d'accéder à du contenu à caractère sexuel sur Internet. Les adresses de ces sites (URL) ne sont pas toujours explicites et peuvent revêtir des aspects anodins à base de mots communs (ex : filles, amour) voire des mots à la mode : star ac, pokemon, etc. De plus, les « bonnes adresses » peuvent se transmettre dans les cours d'école!

L'accessibilité à des sites pédophiles est plus difficile... à moins de tomber dessus par malchance au détour d'un lien inapproprié. Au plus, au cours d'un surf normal, on peut tomber sur des vitrines payantes (.com) proposant des photos... mais pour voir plus il faut payer l'entrée au site. Des réseaux de pédophiles existent et les membres de ces derniers s'échangent des adresses (URL), des photos via les Newsgroups, des BBS, des canaux de Chat et grâce à des logiciels de Peer to Peer. Même bien cachée, cette matière est présente sur Internet et son contenu est très traumatisant.

2) Cas des groupes de discussion (Newsgroups)

Ces groupes sont des « forums de discussion » hébergés par des serveurs de News et dont les sujets portent sur des thèmes les plus variés. Les participants à ces forums y apportent leur contribution sous forme de commentaires écrits. Dans un forum, il se crée alors des fils de discussion de type questions/réponses.

La plupart du temps, ces groupes de discussion sont « modérés » c'est-à-dire qu'une personne (le modérateur) censure tout ce qui ne traite pas du sujet, illégal, contraire à l'éthique du groupe... c'est la théorie.

En pratique, il y a des Newsgroups dont les thèmes sont inappropriés ou alors le thème est approprié mais le filtrage par le modérateur n'est pas satisfaisant. On peut alors lire des propos qui peuvent offenser les enfants ou proposer des échanges de photos ou d'autres matériels.

3) Cas des messageries instantanées et des chats (IRC)

La messagerie instantanée est une fonctionnalité rentrée dans les mœurs des jeunes et des moins jeunes internautes pour créer et maintenir des contacts. C'est le SMS de l'Internet! Elle permet un dialogue écrit en temps réel entre deux personnes. Le succès de ces outils est tel que les utilisateurs de ces derniers sont extrêmement sollicités par des rabatteurs de sites pornographiques

L'IRC est un protocole qui permet de dialoguer en direct. Les messages échangés dans ces canaux de discussion (Chat) sont lus par toutes les personnes qui participent à la discussion. On participe aux chats grâce à des logiciels comme mIRC qui permettent même des discussions en privé entre deux participants. À l'instar des Newsgroups, il en existe sur tous les sujets possibles. Les canaux concernant des discussions hard sont très représentés et leurs titres sont assez explicites pour qu'il n'y ait pas d'ambiguïté sur les sujets de conversation qui sont abordés.

4) Cas des logiciels « Peer to Peer »

Le Peer to Peer est une technologie qui permet de mettre en connexion les ordinateurs des internautes en un véritable réseau d'échange de données. Les internautes partagent ainsi une partie de leur disque dur grâce à des logiciels comme eMule, Kazaa, eDonkey, etc. Ce réseau dans le réseau Internet échange toutes sortes de fichier audio MP3, fichier vidéo DivX et WMA, applications... et matériels pornographique en tous genres. Souvent il installe différent « spyware » ou programme indésirable difficile à supprimer et désagréable.

Comment fonctionne un logiciel de filtrage?

Les logiciels de filtrage s'intercalent entre le navigateur (ou tout autre logiciel) et Internet à moins que le logiciel de filtrage soit à la fois navigateur et logiciel de filtrage; c'est le cas d'AOL 8 et MSN 8.

Pour assurer le filtrage de contenu, l'éditeur du logiciel peut utiliser plusieurs techniques en parallèle :

1) Les bases de données de contenus inappropriés (liste noire de sites)

Dans ce cas, une liste de sites référencés protège l'internaute des sites inappropriés. Elle peut contenir des centaines voire des milliers d'adresses (URL) de pages inappropriées. Cette liste doit être téléchargée régulièrement car elle est mise à jour par l'éditeur du logiciel de filtrage. Les sites de cette liste sont ordonnés en catégories que l'utilisateur peut activer : sexe, pédophilie, violence, racisme, etc.

Le logiciel de filtrage fait alors une comparaison entre l'adresse du site demandé et sa base de données d'URL. Dans le cas d'une similitude d'URL, le logiciel bloque la page du site.

Ces listes sont réalisées en utilisant une ou plusieurs méthodes suivantes :

- Équipe de surfeurs spécialisés qui référencent des sites inappropriés suivant les différentes catégories.
- Agents intelligents qui scrutent l'Internet à la recherche de sites douteux. Puis ces sites sont vérifiés par un surfeur pour évaluer le contenu et être classés dans une catégorie.
- Utilisateurs des logiciels qui font remonter (soumission d'URL) à l'éditeur les URL inappropriées qu'ils ont rencontrées.

Les limites des bases de données d'URL

Le premier problème est la pertinence et l'exhaustivité de cette base de données quand on connaît le nombre exponentiel d'URL mises sur internet. Le second problème est que les moyens humains (type d'experts ? compétences employées pour décider qu'un site est ou n'est pas approprié), les méthodologies et la déontologie mis en œuvre pour mettre une URL dans une liste noire ne sont pas transparents pour les parents utilisateurs.

Quid des listes « blanches »?

La liste noire a son /pendant » que l'on nomme la « liste blanche ». Tout ce qui est dans cette liste est accessible; le reste est bloqué. Cet outil n'est pas à négliger mais son utilisation est vite laborieuse car les sites proposent des liens qui seront alors bloqués. Le concept d'espace « sécurisé » dans laquelle l'enfant évolue sans entrave est semble-t-il plus intéressant.

2) Les listes de mots clés

A l'instar de listes noires d'URL, les éditeurs utilisent des listes de mots à bannir. Ils sont détectés soit dans l'URL du site soit à l'intérieur de la page; pour certains logiciels, leur détection peut être faite dans les moteurs de recherche, les mails, les newsgroups, etc.

Le mot est remplacé par des caractères de substitution (des blancs pour Cybersitter ou des dièses pour Net Nanny, par exemple)... dans ce cas, le reste du message passe ! Autre solution : la page ou le service est bloqué comme avec « don't see! ».

3) Le moteur d'analyse de contenu et de contexte

Ce type d'outil est plus rarement employé car les technologies mises en œuvre ne sont peut-être pas matures voire difficilement « transportables » sur un PC.

Ces moteurs analysent le contenu de la page et les associations de mots pour décider si une page doit être transmise ou non au navigateur.

C'est le cas du logiciel PureSight d'icognito qui filtre en dynamique les sites inappropriés sans avoir recours à une liste d'URL pré-établies. Il fait intervenir « un algorithme utilisant les techniques d'intelligence artificielle » qui permet d'analyser le contenu de la page demandée.

4) Les logiciels d'analyse d'images

Le logiciel analyse le contenu d'une image et détermine si elle est à caractère pornographique ou non. Les pages des sites pornographiques sont affichés, mais les photos sont remplacées par une photo neutre. Le niveau de protection est ajusté à l'aide d'une échelle graduée de 0 à 10.

Dans la pratique, cette analyse est bien réelle mais les résultats sont surprenants : trop de photos de sites pornos passent ou alors, des photos de sites inoffensifs sont bloquées. Il est difficile de trouver un niveau de blocage de photos acceptable... au-delà du fait qu'il ne bloque pas la page porno proprement dite et que le lien de cette dernière, toujours actif, permet d'activer une autre page...

5) Le contrôle d'applications (logiciels de lecture de Newsgroups, de Chat, de FTP, de mail, de Peer to Peer)

Certains logiciels de filtrage permettent de filtrer voire de bloquer l'accès aux newsgroups, aux Chats ou à d'autres applications stockées sur le disque dur.

Dans le cadre du blocage d'application c'est-à-dire de la gestion de l'accès des applications à Internet, l'outil de gestion existe et il s'appelle le pare-feu ou firewall en anglais. Deux logiciels en sont pourvus dans les plus populaires : Norton Internet Security et le McAfee CyberPatrol et Net Nanny permettent également de désactiver « brutalement » toute applications désignées par l'administrateur.

Les navigateurs alternatifs

Les filtrage dans les navigateurs alternatifs : Netscape, Mozilla, Opéra laisse à désirer : ainsi Contrôle kids ne filtre rien dans ces navigateurs, FlowProtector ne filtre pas Mozilla et Opéra, Securitoo ne filtre pas Mozilla...

Des techniques pour solutionné les problèmes

Outil informatique a utilisé

Plusieurs logiciel son disponible sur le Web ou chez nos fournisseurs d'accès Internet. Gratuit, sous-location ou même à faible coût, Ils ne fonctionnent pas nécessairement tous. De cette façon quelque technique vous serons présenté dont un logiciel de contrôle parental, une méthode incluse avec Windows (filtre) ainsi que l'utilisation des log de conversation des logiciels de bavardage.

Pour le logiciel, il s'agit d'un « freeware » et il se nomme « don't see ! ». Voici un petit guide d'utilisation.

Tout d'abord il faut se le procuré, un petit tour sur le site de @robas est une compagnies qui offre des logiciels gratuit au particulier et au compagnie. <http://www.arobas-fr.com/> utilisé le lien téléchargements à la gauche, spécifier le logiciel a télécharger, pour cette atelier il s'agit de « don't see ! » ainsi que du système d'exploitation utilisé, appuyez sur envoyer et par la suite téléchargez. Une fois télécharger, il ne vous reste plus qu'à l'installé.

Comme tout logiciel il faut lancé l'exécutable d'installation et suivre les étapes.

Par la suite lancez « don't see ! ». La première chose à faire est de choisir un mot de passe : cliquez sur l'onglet Sécurité et choisissez un mot de passe. Cela permet de bloquer l'accès au paramétrage du logiciel à toutes les personnes qui ne connaissent pas le mot de passe.

PARAMÉTRAGE DU LOGICIEL

Onglet général :



Il est préférable de lancer « don't see ! » au démarrage, car il n'est effectif que s'il est lancé, bien évidemment. Il est aussi préférable de désactiver le gestionnaire des tâches car sinon il est possible de fermer « don't see ! » en faisant ctrl+alt. +suppr. : le contrôle parental n'aurait alors plus d'effet.

Pour la case Message, c'est au choix. Personnellement je préfère mettre un message, c'est plus clair comme ça. Le message est modifiable, il suffit d'écrire son propre message à la place de celui existant.

Onglet Listes : Détermination de la liste des mots clés à interdire.

Sur la colonne de gauche les mots clés à interdire, sur la colonne de droite, les mots clés autorisés. Personnellement je ne vois pas trop l'intérêt de cette deuxième colonne puisque tous les mots qui ne sont pas interdits sont autorisés.

Une bonne partie du travail est déjà faite car le logiciel comporte déjà une liste de mots clés interdits.

Pour ajouter un mot interdit, tapez le dans le champ de texte. Ensuite vous avez deux possibilités :

- Vous voulez que le mot entré ainsi que toutes ses déclinaisons soient interdits, dans ce cas vous cliquez sur Ajouter ce mot à la liste interdite (la case Ajouter un mot entier ne doit pas être cochée) Ex : vous tapez mot et les mots moto, moteur, motivation... seront interdits
- Vous voulez que le mot exactement entré soit interdit, dans ce cas vous cochez la case Ajouter le mot entier et vous cliquez sur Ajouter ce mot à la liste interdite. Ex : vous tapez mot et les mots moto, moteur, motivation... seront autorisés.

Si vous voulez supprimer un mot de la liste il suffit de double-cliquer dessus.

Vous pouvez voir les pages qui ont été fermées par « don't see ! » en cliquant sur l'onglet pages fermées.

Onglet Mise a jour :

Cliquez sur Vérifier les mises à jour de « don't see ! » maintenant pour voir s'il existe une version plus récente que celle que vous avez. Si une nouvelle version existe, un message vous demande si vous voulez l'installer. Si vous cliquez sur oui, vous êtes dirigé vers le site de l'auteur de « don't see ! ». Choisissez de télécharger la version de « don't see ! » qui correspond à votre système d'exploitation.

Avant d'installer la nouvelle version, il faut désinstaller celle que vous avez déjà sur votre ordinateur.

Microsoft offre inclus dans Windows quelques possibilité pour faire un contrôle de base, nous avons pour commencé les filtres qui son disponible dans toute les version d'Internet Explorer. La méthode pour obtenir la fenêtre de contrôle est simple mais l'utilisation n'est pas pratique si nous n'utilisons pas un logiciel pour « logger » les sites Web que votre enfant ou même vous même avez visité (en langage simple il faut commencé par connaître des site Web que vous désirez interdire pour pouvoir les bloqués).

Une foi dans Internet Explorer, dans la bar de menu, faire un simple clic sur Outils, un menu apparaîtras, sélectionné Option Internet dans ce même menu. Dans la fenêtre qui ouvrira sélectionné l'onglet Sécurité par la suite un simple clic sur Sites sensibles. A cette étape il ne reste plus qu'à cliquer sur le bouton Sites qui lui vous ouvrira une autre fenêtre dans lequel vous pourrez entré les adresses des sites Web que vous désirez bloquer.



Astuces : il serait avantageux pour utilisé cette méthode de faire quelque recherche sur des moteurs de recherche tel que : www.google.ca www.altavista.com www.yahoo.com www.yahoo.fr ainsi que le moteur sur le site <http://symatico.msn.ca/> à l'aide de mot clé et d'utilisé une banque de mot clé pour faire des recherche et par la suite entré les sites retrouvé dans l'option des sites sensibles. Banque de mot clé :

@priv, 100sex100, 1ero68, 3xmania, adult, adult cinema, adultos, adults only, anal, asian, ass, baise, bang, bdsm, beast, before you go, bestiality, big movie, big naturals, big sauvage pizza, bigmovie, bite, blonde, blow job, blowjob, bonda, briana, brune, bukkake, busty, carpediem, charme, chatte .com, chillin' chicks, clara, cock, constantina, coquin, coquine, cream of da crop, cul, cuni, dans movies, dansmovies, deep throat babes, dildo, dvdx, ebony babes, edonkeymaster, ejac, ejacs, enter!, eroti, espotting, etudiante .com, etudiante.com, etudiantesx, exhib, extace-x, fantams, farmsecrets, fellation, fesse, feti, filmx, filmxxx, first time, first time auditions, firsttime, free access pass, free movie, freemovie, fuck, gallery, gangbang, gay, girl-girl lovers, girliezoo, gloryholestation, gode, gueb, hand job, handjob*, hard, hentao, humour, hunt, imlive.com, in the vip, instant access, internal, inthevip, jizzled, juicy, kaan, karas, latinax, leamovies, ledortoire, lesbian, lesbiennes, lesbo rama, libid, livedestar, lolita, m.i.l.f., mangas xxx, mangax, maso, masturbating, mature, megatitty, milf, morgan, mouthfuls, movie-machine, moviesguy, mr12inch, naked, naughty, nichon, nichons, nudité, nue, oralsex, orgasm, orgy, pénétration, pénis, photox, pimp, pipe, pissing, playthingz, porn, porno, priv .ocm, pute, rami's movies, rotten, rousse, sabjoli, sado, salope, sample movie, samplemovie, sectionx, seins, sex, sexe, sexy, sinclair, sluts, sluttoons, sodomi, sperm, suck, swallows, t e e n, tabata, twanee, taxi cam, teachers in action, teen, titty, toon movie,

toonmovie, topfrancophone, trans, ultra blue, untitled, video x, videopost, video-post, video xxx, videox, vidsearch, we live together, welivetogether, xx0, xxx, et zoophil.

Note : *cette liste peu être imprimé et distribuer au personne assistant à l'atelier, c'est la liste par défaut du logiciel, il peu s'ajouté des mots.*

Dans la même suite d'idée, nous pouvons configuré et activé les filtres d'Internet Explorer se trouvant dans la fenêtre des Options Internet. Pour accéder au Gestionnaire d'accès, il faut ouvrir Internet Explorer et aller dans l'**Outils**, puis **Options Internet...** et sélectionner l'onglet **Contenu**. Cliquez sur **Activer...** et vous voilà dans le gestionnaire d'accès.

- Pour commencer, saisissez un mot de passe : onglet **Général**, puis **Modifier le mot de passe...** Vérifier par la même occasion que la cas « Les utilisateurs peuvent visiter les sites sans contrôles d'accès » n'est **pas** cochée.
- Sélectionnez maintenant l'onglet **Contrôle d'accès**. Vous pouvez ici choisir très précisément le type de contenus que les utilisateurs seront autorisés à découvrir. **Mais attention! Toutes les pages Web sont loin d'être référencées! (Il doit avoir un certificat pour être référencées, seul les sites d'envergure possèdent de tel certificat habituellement.)** **Si une page est référencée**, le contrôleur comparera les critères de la page et ceux que vous avez déterminés. Si ils correspondent, il autorisera l'accès.

Si une page n'est pas référencée, le navigateur refusera systématiquement l'accès et demandera votre mot de passe. Ainsi, vous et vous seul(e) décidez d'autoriser ou non l'accès à un site, accès qui peut être temporaire (pour évaluation) ou permanent (le site est alors automatiquement ajouté à la liste des sites autorisés, voir ci-dessous)



- L'onglet **Site autorisés** vous permet d'affiner encore votre sélection. Indépendamment

du contrôle d'accès, vous pouvez ainsi autoriser ou interdire complètement l'accès aux sites de votre choix. Après avoir vérifié qu'un site répond à vos critères, vous pouvez l'ajouter à la liste et construire petit à petit une bibliothèque de sites sans dangers pour vos enfants...

Important : le gestionnaire d'accès est utile... si vous n'oubliez pas de l'activer!

Pour l'utilisation des log de chat, il serait avantageux des les consulté uniquement en dernier recourt car une jeune pourrait être offensé dans sa vie privé. Les plus alertes son au courent de l'existence de c'est log, il les auront peu être déjà désactivé.

Débutons avec MSN, pour toute les versions il se crée un dossier historique, à l'emplacement suivant : pour les version 9x, c:\Mes documents\Mes fichier reçus\compte msn\historique et pour les version XP c:\Documents and Settings\le nom d'utilisateur\Mes documents\ Mes fichiers reçus\compte msn\historique. Advenant le cas ou l'enregistrement des conversations ne serai pas activé, il peu l'être à l'aide du menu Outils/options... dans msn. Par la suite dans l'onglet messages, il suffit de coché la case dans historique de conversation (l'emplacement de l'historique peu être modifier a la guise de l'utilisateur).

Pour ce qui est des log d'IRC... Il vous suffit de trouver l'emplacement d'installation du logiciel. Habituellement il se trouve dans c:\Program File\mIRC\log\, encore la il a pus être installé a un endroit différent. Si le dossier est vide la méthode pour les activer est la suivante. Dans les option de mIRC ouvrir l'arborescence IRC et allé dans loggin