



LES DEUX VISAGES D'INTERNET

espionnages, logiciels libres, cookies, spams, antivirus, logiciels libres, blogs, réseaux sociaux, comportements addictifs ...

2012

un document numérique réalisé par le Centre Information Jeunesse Aquitaine



grâce au soutien de





L'horizon infini

Internet ouvre à chacun les voies de l'universalité. Universalité de la toile mondiale. Universalité des thèmes qui y nichent. Universalité des publics que le village mondial draine, dans toute la richesse des diversités culturelles, politiques, religieuses, philosophiques...

Mais il y a les faux nez. Il y a les indéliçats qui proposent des bonbons avec leurs grands imperméables. Sous les artifices de l'utilité peuvent se cacher de redoutables dangers, des individus douteux, voire des réseaux.

Ce guide a pour objet d'aider à débusquer les duperies, les piratages, les escroqueries, les virus... Pour s'en prémunir et protéger les jeunes. Afin d'ouvrir grandes les portes de la foulditude de bienfaits et d'enrichissements offerts par le net : dialogues, confrontation des cultures, logiciels libres, insertion, mobilité, Information Jeunesse...

Pascal JARTY
Directeur du CIJA

LES DEUX VISAGES D'INTERNET



Président : Jean-Charles LAMOULIATTE
Directeur : Pascal JARTY

Document conçu et réalisé par le
Centre Information Jeunesse Aquitaine
5, rue Duffour Dubergier - 125, cours Alsace et Lorraine
33000 BORDEAUX
Tél : 05 56 56 00 56 - Fax : 05 56 52 83 21
www.info-jeune.net

Documentation :
Daniel AUCLERT (CIJA Bordeaux)

Dépôt légal à parution

LES ENFANTS SUR INTERNET

Formidable source d'information, Internet contient le meilleur et le pire. On se doit de protéger les plus jeunes internautes contre certains contenus ; pornographie, propos illicites, incitations à la violence ou au racisme, etc ...

Il est possible de se protéger en utilisant des logiciels de filtrage, en signalant certains contenus ou en portant plainte auprès des autorités.

• Les logiciels de filtrage

Les logiciels de filtrage comme Optenet Webfilter, en téléchargement gratuit sur www.education.optenet.fr, CyberPatrol ou Cybersitter (payants) permettent d'interdire l'accès à certains sites ou à certains types d'informations.



Leur fonctionnement est simple : on peut soit interdire l'accès aux sites répertoriés sur une «liste noire», soit refuser les adresses ou contenus comportant des mots indésirables.

Toutefois, le filtrage par mots-clés présente l'inconvénient de bloquer aussi l'accès à des sites dont le contenu n'est pas toujours préjudiciable.

• A noter :

Sur www.logprotect.fr, vous trouverez un logiciel de contrôle parental libre et gratuit qui a pour but d'empêcher l'enfant de donner ses coordonnées personnelles sur Internet.

Il existe aussi des systèmes de filtrage intégrés dans les logiciels de navigation (Internet Explorer, Firefox, etc...).

On peut les régler selon différents "niveaux de sécurité". Mais l'efficacité est limitée par le faible nombre de sites référencés.

Les logiciels de filtrage permettent donc de "sécuriser" partiellement la navigation sur Internet pour les plus jeunes, mais ils sont loin d'être infaillibles et ne peuvent se substituer totalement à la vigilance des adultes.

• Les Services que l'on peut contacter

Le site de l'**AFA** (Association des fournisseurs d'accès et de services internet) :

www.pointdecontact.net, par exemple, informe sur les textes de loi applicables en matière de pédophilie et d'incitation à la haine raciale. Vous y trouverez aussi une aide pour identifier les sites illicites, et vous pourrez signaler des contenus illicites à l'AFA, qui transmettra l'information à l'OCLCTIC ... (Office central chargé de la lutte contre la criminalité liée aux technologies de l'information et de la communication).

D'autre part, vous pouvez aussi signaler les contenus illicites directement à l'OCLCTIC sur le site :

internet-signalement.gouv.fr

LES ENFANTS SUR INTERNET



L'**OCLCTIC** appartient à la Direction Générale de la Police Nationale et dépend de Direction Centrale de la Police Judiciaire. Cet organisme a été créé afin de lutter contre la délinquance liée aux nouvelles technologies de l'information et de la communication.

- **Porter plainte**

Lorsque l'on découvre des contenus illégaux ou préjudiciables, on peut bien sûr porter plainte (police ou gendarmerie), ou contacter L'OCLCTIC :

**INFO ESCROQUERIES
(OCLCTIC)
08 11 02 02 17
(Prix d'un appel local)**

GENDARMERIE NATIONALE
www.gendarmerie.interieur.gouv.fr

Attention :

il ne s'agit pas de se rendre coupable de "dénonciation calomnieuse" (articles 226-10 et suivants du Code pénal) en portant plainte contre une personne nommément désignée. La "dénonciation calomnieuse" peut être punie par la loi (emprisonnement + amende).

- **Services publics pour la protection de l'enfance**



- **119 - Allô Enfance En Danger**
www.allo119.gouv.fr

- **Le Défenseur des Droits** est une autorité constitutionnelle indépendante qui veille à la protection de vos droits et de vos libertés. Elle est, entre autres, chargée de défendre et de promouvoir les droits de l'enfant :
<http://defenseurdesdroits.fr/connaitre-son-action/la-defense-des-droits-des-enfants>

- **Le Ministère des Solidarités et de la Cohésion Sociale** propose également sur son site solidarite.gouv.fr une information à destination des familles.

- **A voir aussi sur Internet ...**

Le **CLEMI** (Centre de Liaison de l'Enseignement et des Médias d'Information), rattaché au Ministère de l'Éducation Nationale, conçoit et diffuse des programmes d'éducation aux médias : www.clemi.org.





DEVELOPPONS ENSEMBLE
L'ESPRIT D'EQUIPE SOCIÉTÉ GÉNÉRALE

SOCIÉTÉ GÉNÉRALE

Partenaire de l'UGC Ciné Cité de Bordeaux



10 PLACES
DE
CINÉMA UGC
OFFERTES⁽¹⁾



SERVICES
BANCAIRES⁽²⁾
1€
PENDANT 1 AN

à l'ouverture d'un 1^{er} compte bancaire

Mentions légales: (1) Dix places d'une valeur unitaire de 5,50€ ainsi qu'une carte UGC Blue d'une valeur de 2€ (tarifs susceptibles d'être modifiés). Les places de cinéma offertes sont valables quelque soit la séance et uniquement à l'UGC Ciné Cité Bordeaux, 13-15 rue Georges Bonnac, 33000 Bordeaux. Offre non cumulable, réservée aux 16-24 ans non détenteurs d'un compte bancaire à la Société Générale, valable dans toutes les agences Société Générale de Gironde et de Biscarrosse, pour toute ouverture de compte jusqu'au 31/06/2012. Ouverture de compte sous réserve d'acceptation de votre dossier Société Générale par la banque. Les mineurs doivent être accompagnés par leur représentant légal. La carte UGC Blue vous sera créditée de dix places au total: cinq places à l'ouverture de votre compte, et cinq places supplémentaires six mois plus tard si le compte est actif, c'est à dire si l'enregistre au moins cinq opérations par mois pendant six mois. (2) Services bancaires inclus dans Jazz. Offre réservée aux 16-24 ans. Tarifs Jazz en vigueur au 01/02/12, hors offre privilège: avec une Carte Bleue nationale ou Carte V-Pay: 1,78€/mois pour les 16-17 ans et 3,55€/mois pour les 18-24 ans - avec une Carte Bleue Visa ou Carte Mastercard: 1,88€/mois pour les 16-17 ans et 3,75€/mois pour les 18-24 ans - avec une Carte Visa Premier ou Carte Gold Mastercard: 7,40€/mois pour les 18-24 ans - avec une Carte Visa Infinite: 28,50€/mois pour les 18-24 ans.

Société Générale - SA au capital de 970 099 988,75 euros - 552 120 222 RCS Paris, Siège social 29 boulevard Haussmann - Représentée par le Directeur d'Exploitation Commerciale de Bordeaux au 28 Cours de l'Intendance 33000 Bordeaux.

LES DANGERS DU CHAT

Les messageries instantanées



Le "**Chat**" est un lieu de conversation sur Internet où les internautes communiquent entre eux en temps réel, par l'intermédiaire de messages textuels. Endroit de communication et de rencontres, c'est surtout un terrain privilégié où les jeunes peuvent s'exprimer et échanger avec leurs pairs.

Au sujet des sites de chat, la presse, regorge de faits divers sur fond de pédophilie et de prostitution mais, au-delà de cette vision alarmiste, il faut aussi considérer les atouts de ce mode de communication quasi instantané.

Discuter "en direct" avec les copains, un parent éloigné, une personnalité, ou un employeur potentiel, ... les attraits du chat ne manquent pas.

Mais ces usages, légitimes et utiles, ne doivent pas faire oublier les dangers. Si le chat n'est pas la cause de tous les maux, il facilite néanmoins la prise de risque pour celui ou celle qui est mal informé ou mal préparé.

En effet, **le CHAT facilite l'anonymat** ; un "chatter" peut en cacher un autre et il faut prendre soin de préserver ses informations personnelles.

• Comment fonctionne un "Chat" ?

En général, n'importe qui peut s'inscrire dans un Chat et il n'y a aucun contrôle de l'âge des participants. La plupart du temps, il suffit de donner un faux nom (pseudonyme) pour être accepté.

Une fois inscrit, il est possible de dire à peu près tout et n'importe quoi sur un chat. Heureusement, de plus en plus, les services de Chat sérieux proposent un contrôle et rejettent ou interdisent les conversations douteuses.

Le Chat permet donc à chacun de se choisir une identité fictive pour s'exprimer. C'est là tout le charme ... et aussi le danger du chat ; on ne voit pas son interlocuteur et l'on ne perçoit de lui qu'un pseudo et ce qu'il tape au clavier...

Pour les ados, l'attrait est grand : on peut y oublier les parents, l'école et les problèmes, on y trouve un nouvel espace de liberté.

C'est le lieu où l'on s'imagine un monde à soi et où l'on se présente tel que l'on voudrait être...

Et c'est d'autant plus facile que la déconnexion de la réalité est immédiate ; il suffit d'allumer son PC.

Mais celui qui utilise les messageries instantanées doit être responsable de ce qu'il dit, rester vigilant quand aux risques et ne pas trop oublier la réalité pour être en mesure de résister aux influences et aux manipulations.

• Les précautions à prendre sur le chat

Pour les plus jeunes, un certain nombre de précautions permettent de chatter en toute sécurité :

- Ne pas communiquer son adresse sur les chat et sur les forums.
- Ne pas communiquer son numéro de téléphone ou sa photo.
- Ne pas s'identifier avec son vrai nom.
- Ne pas aller à un rendez-vous "IRL" (In Real Life = "dans la vie réelle") sans être accompagné d'un adulte.
- Ne pas communiquer son adresse email à des étrangers.

• **Interrompre immédiatement une conversation chat qui prend un caractère pornographique, porte atteinte à la pudeur ou devient trop indiscreète.**

Dès que les enfants ressentent un malaise, il serait souhaitable qu'ils en parlent avec leurs parents ou avec un adulte de confiance.

Et si le chat dispose d'un service de modération, il ne faut pas hésiter à l'avertir dès que l'on constate des conversations bizarres.



Les publicités non sollicitées, pétitions, chaînes de lettres, fausses alertes aux virus (hoaxes), arnaques bancaires inondent nos boîtes aux lettres électroniques.

Les "Spams", ou courriels abusifs, se caractérisent par leur quantité, le fait qu'ils soient envoyés sans le consentement du destinataire et leur contenu inutile, choquant ou préjudiciable.

Ils ralentissent le réseau et obligent les utilisateurs à faire le tri, à réception, entre le bon grain (souvent pas plus de 10% des courriers reçus) et l'ivraie.

• Les Spams et la loi ...

Le Parlement Européen a adopté une directive spécifique concernant le spam et l'envoi de courriers électroniques non sollicités, en faveur de l'opt-in (consentement préalable des internautes), en juillet 2002.

Au regard des législations existantes en France et des directives européennes mises en place, un constat s'impose :

Le spam est illégal en France et en Europe.

VIVONS LA VILLE de DEMAIN



BORDEAUX
Ma ville

**Semaine
DIGITALE**

**23 mars
1^{er} avril**

bordeaux.fr



SE DEFENDRE CONTRE LES SPAMS

En France, la **Commission Nationale de l'Informatique et des Libertés** mène depuis plusieurs années une politique active de lutte contre le spam, qu'il s'agisse de l'application effective de la législation anti-spam, de l'adoption de codes de bonne conduite par les professionnels, ou encore du développement d'une forte coopération internationale.

Il faut savoir que les prospecteurs commerciaux sont tenus de rendre les publicités identifiables de manière claire et non équivoque dès leur réception et ils doivent arrêter les envois non sollicités dès vous leur avez signifié votre refus de figurer parmi leurs destinataires.



De plus, ils ne sont pas autorisés à collecter des données personnelles via Internet à l'insu de l'internaute. Seules les adresses loyalement collectées, par exemple lors d'une transaction commerciale, peuvent être utilisées à des fins de sollicitations directes par courrier électronique en France (Loi "Informatique et Libertés" et Directive européenne sur la "protection des données à caractère personnel").

Les publicitaires doivent déclarer la collecte et l'enregistrement d'informations nominatives auprès de la CNIL. Ils ont obligation d'informer l'internaute de l'utilisation qui sera faite de ses coordonnées et ce dernier doit pouvoir s'opposer au traitement de ses données personnelles.

Pour en savoir plus :

www.cnil.fr

• Comment se protéger des Spammeurs ?

Des solutions existent et voici quelques conseils pour "limiter la casse" :

1) Evitez de répondre aux spams, car cela permet à l'expéditeur de vérifier la validité de votre adresse électronique avant de l'utiliser à nouveau ou de la revendre.

2) Evitez de faire figurer votre email habituel sur des sites web ou des groupes de discussion. Elle peut être récupérée par un logiciel de collecte pour constituer la "mailing-list" d'un spammeur.

Utilisez plutôt une adresse auxiliaire ou cryptez votre adresse habituelle. (voir aussi la solution proposée par MailPatch : <http://mailpatch.com/fr/>)

3) Evitez de donner votre adresse mél si vous ne savez pas l'utilisation qui en sera faite (le cas échéant, se renseigner sur le sérieux de l'organisme qui vous la demande).

• On peu aussi filtrer les Spams

La plupart des logiciels de courrier électronique (Windows Mail, Thunderbird, Outlook) permettent de filtrer les courriers entrants en fonction de mots-clés ou de l'adresse de l'expéditeur.

Il existe aussi des logiciels dédiés, dits «Anti-spams» qui peuvent faciliter le tri du courrier comme :

• **Vade-Retro** (payant) : <http://www.vade-retro.com/fr/>

- **SpamBayes** (logiciel libre) : <http://spambayes.sourceforge.net/>



Partenaire du réseau Tbc

+ de 5 mensualités
offertes de votre abonnement Tbc

soit 85 €⁽¹⁾,

pour toute ouverture d'un compte bancaire
et d'un livret d'épargne



Services bancaires⁽²⁾ à
1 €/an pendant 2 ans.

Pour
les abonnés
Pass'
Jeune
TbcTM

Pour bénéficier de cette offre, présentez-vous dans l'une des **agences Société Générale** de Gironde et Biscarrosse. Retrouver l'agence la plus proche de chez vous sur jeunes.societegenerale.fr.

Informations sur infotbc.com ou au **05 57 57 88 88**



Mention légales : (1) Offre valable jusqu'au 31/06/2012 dans toutes les agences Société Générale de Gironde et Biscarrosse, et réservée aux détenteurs de l'abonnement Pass' Jeune Tbc âgés de 16 à 24 ans à l'ouverture d'un premier compte et/ou d'un livret d'épargne à la Société Générale. L'ouverture du compte à vue et la souscription d'un Livret d'Épargne (Livret Jeune, Livret A, Épargne Junior, PEL...) présentés dans l'offre sont soumises à l'acceptation de la banque et supposent, préalablement, la signature de contrats remis en agence le jour de l'adhésion. La somme de 85€ sera versée sous réserve que le compte ait enregistré au moins 5 opérations de débit ou de crédit par mois pendant 6 mois et sera divisée en deux: 60 € sur le compte à vue et 25 € sur le livret. La Société Générale peut vous envoyer gratuitement les Conditions Générales. Vous bénéficiez, pendant 14 jours à compter de la date de conclusion du contrat, du droit de vous rétracter, et ce, au moyen d'un simple écrit remis par tout moyen à votre agence. Il vous appartient de conserver la preuve d'une telle remise (par exemple, visa d'un agent Société Générale). La présence du représentant légal est obligatoire pour l'ouverture d'un compte à un mineur. (1) Ouverture du compte à vue sous réserve d'acceptation par l'agence. Le mineur doit être accompagné de son représentant légal. Les intérêts dépendent du livret souscrit. Le mineur doit être accompagné de son représentant légal. (2) Offre réservée aux personnes de 16 à 24 ans. Remboursement annuel de Jazz sous réserve de présentation au conseiller de la carte TBC à la date d'anniversaire de sa souscription. Cotisation mensuelle hors promotion: avec une Carte Bleue nationale ou Carte V-Pay: 1.78€ pour les 16-17 ans et 3.55€ pour les 18-24 ans; avec une Carte Bleue Visa ou Carte Mastercard: 1.88€ pour les 16-17 ans et 3.75€ pour les 18-24 ans; avec une Carte Visa Premier ou Carte Gold Mastercard: 7.40€ pour les 18-24 ans et avec une Carte Infinite: 28.50€ pour les 18-24 ans. Tarif en vigueur au 01/02/12.

DEVELOPPONS ENSEMBLE
L'ESPRIT D'EQUIPE  SOCIETE GENERALE

- **Enfin, on peut dénoncer les courriels abusifs**

Il n'est pas toujours aisé d'identifier l'expéditeur d'un courriel abusif. Ce dernier peut d'ailleurs déjouer les techniques de filtrage en changeant systématiquement d'adresse d'envoi.

Vous pouvez signaler à la CNIL les courriels qui ne respectent pas les dispositions légales via le site de l'association Signal-spam :

www.signal-spam.fr



Vous pouvez aussi **signaler les messages abusifs auprès de votre fournisseur d'accès**, ce qui lui permettra d'opérer un filtrage généralisé pour l'ensemble de ses abonnés.

Pour cela, il faut lui envoyer par mail une copie de l'en-tête du courrier abusif.

Traque sur Internet !

Nom, adresse, n° de carte bleue, e-mail, n° de téléphone, etc ...

Sur Internet, il est très facile de dévoiler, à son insu, des éléments de sa vie privée.

- **Pourquoi sommes-nous espionnés?**

- Pour des raisons commerciales : on veut connaître nos goûts et nos habitudes de consommation, pour nous vendre quelque chose ou vous envoyer des publicités.

- On veut nous empêcher de pirater des logiciels : les éditeurs de logiciels utilisent Internet pour détecter d'éventuels logiciels piratés sur notre ordinateur (pour essayer de nous convaincre de les acheter ou, au pire, pour nous traîner en justice).



- **Comment ça marche?**

1) Une personne mal intentionnée peut, en ayant accès à des mots de passe de connexion, intercepter des mails ou visiter des bases de données contenant des informations confidentielles (n° de carte bleue, ... heureusement, la loi française protège l'utilisateur qui est victime d'une utilisation frauduleuse de sa carte).

Pour éviter ce genre d'ennui, on peut crypter ses mails : c'est à dire les protéger en utilisant un logiciel d'encodage comme **OpenPGP** :

<http://openpgp.vie-privee.org/>

RESTER MAÎTRE DE SON IDENTITÉ SUR LE NET

2) Les sites commerciaux utilisent les "cookies" pour connaître les habitudes de navigation de l'utilisateur, les sites et moteurs de recherche qu'il utilise, l'ordinateur et les logiciels qu'il emploie ou toute autre information qu'il accepterait de déposer dans un formulaire à remplir via Internet.

3) Les fournisseurs d'accès à Internet payants disposent de fichiers très complets : Coordonnées électroniques, bancaires et postales. (Les FAI gratuits, eux, ne possèdent généralement que vos coordonnées électroniques).

4) Des logiciels installés sur votre disque dur peuvent, lorsque vous êtes connecté, transmettre des informations vous concernant, pour savoir si les programmes que vous utilisez sont piratés.

5) Des techniques d'observations basées sur l'indiscrétion des navigateurs Web (Internet Explorer et autres...) permettent de collecter des informations sur l'internaute (cookies, fichiers temporaires, etc.). On peut ainsi recueillir des informations sur l'internaute (langue, pays de connexion, fournisseur d'accès, adresse IP, habitudes de navigation, adresses électroniques etc.) et les utiliser à des fins commerciales ou discriminatoires.

6) Il existe aussi des outils spécialisés et plus pernecieux : les espioniciels (ou Spywares). Ces logiciels-espions sont programmés pour voler diverses informations directement sur le disque dur de l'utilisateur.

Les cookies

Un cookie (ou "mouchard électronique") est un petit fichier texte installé par votre navigateur sur votre disque dur à la demande d'un site au moment où vous le visitez.

Les cookies permettent de "reconnaître" un visiteur en recueillant des éléments d'identification : adresse IP, système d'exploitation, navigateur utilisés, navigation effectuée sur le site... S'ils ne contiennent pas forcément des données privées, les cookies permettent de connaître vos habitudes de navigation.

Les cookies peuvent aussi être très utiles et faciliter la navigation de l'internaute en rappelant les préférences qu'il a pu déclarer lors d'une précédente visite sur un site (identifiant, mot de passe, etc...).

Malheureusement, ils sont aussi utilisés par les publicitaires afin d'adapter des annonces vos préférences (publicité dite "comportementale").

• Gérer les cookies

On peut les gérer en configurant son navigateur pour qu'il avertisse lorsqu'un site demande la création d'un cookie ou pour qu'il refuse systématiquement tous les cookies.

On peut aussi éliminer les cookies déjà stockés : (Attention, certains cookies contiennent des informations qui vous permettent d'être automatiquement identifié sur un site et de délivrer votre mot de passe. Ne les effacez pas si vous n'êtes pas certain d'avoir noté tous les identifiants et mots de passe qui vous permettent d'utiliser un service sur l'internet).

RESTER MAÎTRE DE SON IDENTITÉ SUR LE NET

La plupart des navigateurs actuels propose une gestion précise des cookies à l'aide des "Préférences" ou des "Options Internet" : on peut les effacer, les filtrer ou les refuser.

Le site de la CNIL explique le fonctionnement des cookies de manière très claire grâce à une petite démonstration "en ligne", à l'adresse suivante :

www.cnil.fr/vos-libertes/vos-traces/

Lutter contre les espioniciels

Les spywares, logiciels espions et autres espioniciels sont des petits programmes qui sont souvent intégrés ou livrés en complément d'un logiciel principal.

Ils s'installent sur l'ordinateur à l'insu de l'utilisateur et collectent des données sur l'internaute et sa machine.

L'espioniciel transmet ces données à son créateur, la plupart du temps à des fins publicitaires et commerciales.

Les espioniciels sont souvent associés à des logiciels proposés en téléchargement gratuit sur le Net (logiciels d'échanges de fichiers peer-to-peer ou clients de messagerie instantanée). Mouchards électroniques aux fonctionnalités étendues, ils peuvent envoyer dès le démarrage de l'ordinateur vers les serveurs d'un organisme "maître" toutes les données qu'ils y ont collectées : adresses électroniques, mots de passe enregistrés, etc.

L'objectif affiché par les éditeurs de ces logiciels est d'assurer une meilleure maintenance des programmes dans lesquels ils sont intégrés (envoi automatisé à l'utilisateur les correctifs indispensables au bon fonctionnement du programme).

Mais, malheureusement, les données ainsi collectées sont le plus souvent revendues à des régies publicitaires.

• Se débarrasser des espioniciels

• **Faire attention à ce que l'on installe sur son ordinateur** (surtout si c'est gratuit!).

Lors de l'installation de logiciels téléchargés, **lire attentivement les boîtes de dialogue et désactiver les modules additionnels** qui ne sont pas indispensables au bon fonctionnement du programme.

• **Lire le CLUF (Contrat de Licence d'Utilisateur Final)** qui mentionne parfois les spywares inclus dans le logiciel que l'on va installer.

• **Effectuer des diagnostics réguliers et surveiller sa machine : Un Anti-virus et un Pare-feu (firewall) peuvent être utiles.** Le pare-feu permet d'être alerté lors des tentatives de connexion à des serveurs distants, mais son efficacité est limitée car il vérifie surtout données entrantes. Celle des anti-virus l'est tout autant car les espioniciels sont rarement identifiés comme des virus.

• **Procéder à des nettoyages réguliers** : Le moyen le plus efficace de se prémunir contre les espioniciels est d'avoir recours à des programmes spécialisés pour les identifier et les détruire. Il existe plusieurs **programmes anti-spyware**, disponibles sur Internet, comme le logiciel **Ad-Aware**, qui fonctionne très bien (www.lavasoft.com).



RESTER MAÎTRE DE SON IDENTITÉ SUR LE NET

AUTRES LOGICIELS D'ESPIONNAGE :

**Javascrpts,
applets Java,
contrôles ActiveX**

Les **Javascript** sont des programmes intégrés dans le code HTML de la page et exécutés directement par le navigateur.

Les **Applets java** sont des mini-applications autonomes qui effectuent des tâches spécifiques dans le site web sur lequel elles sont intégrées.

Les **Contrôles ActiveX** (technologie Microsoft), sont aussi des mini-applications qui sont téléchargées et exécutées directement par le navigateur.

Ces applications peuvent déclencher l'ouverture de fenêtres publicitaires (popups) ou inscrire un site en page de démarrage (home) du navigateur.

Elles peuvent aussi collecter des données personnelles (configuration de la machine, historique des sites visités, adresses électroniques...).

Comment se défendre ?

Gérer les contrôles ActiveX : Dans le menu "Options" du navigateur, l'onglet "Sécurité" permet de définir un niveau de protection pour les Contrôles ActiveX et des plug-ins.

Gérer les scripts java dans le navigateur : Les "préférences" ou le menu "option" permettent de régler les paramètres des scripts et, par exemple, de désactiver l'ouverture de "pop-ups" lors de la navigation.

• Les indiscretions de votre navigateur...

Les navigateurs permettent de visualiser des contenus disponibles sur des serveurs distants.

Lorsque l'on saisit l'adresse d'un site, on envoie de nombreuses informations au serveur distant : protocole, serveur à contacter, document demandé, marque et n° de version du navigateur, adresse IP locale, présence d'un cookie appartenant au site visité, etc.

Heureusement, **on peut, dans une certaine mesure, maîtriser les données envoyées par le navigateur :**

Pour **surfer anonymement**, activez la "navigation privée" ou utilisez un site d'anonymat qui masquera les informations vous concernant.

De la même façon, **le courrier électronique peut être rendu anonyme** par la suppression des en-têtes.

Pour en savoir plus, consultez le site d'arobase.org :

www.arobase.org/confidentiel/anonym.htm



VIVONS LA VILLE de DEMAIN



BORDEAUX
Ma ville

**Semaine
DIGITALE**

**23 mars
1^{er} avril**

bordeaux.fr



CREER UN SITE WEB OU UN BLOG

Ce qu'il faut faire !

- **Enregistrer son nom de domaine**

Pour être mieux identifié sur Internet, il est souhaitable enregistrer son nom de domaine en s'adressant à l'un des services suivants :

1) AFNIC, www.afnic.asso.fr pour les noms de domaine en .fr, .asso.fr (Association Française pour le Nommage Internet en Coopération)

2) INTERNIC, www.internic.com pour les noms de domaine en .com, .net, .org, ...

3) EURID, www.eurid.eu/fr/ pour les noms de domaine en .eu

Attention : Le Code de la propriété intellectuelle protège le titulaire d'une marque qui a été enregistrée auprès de l'INPI (Institut National de la Propriété Industrielle), mais il ne protège pas le nom de domaine.

Si l'on ne possède pas la marque que l'on veut faire apparaître dans le nom de domaine, il faut vérifier que le nom en question n'entre pas en conflit avec une marque existante, et il vaut mieux enregistrer la marque auprès de l'INPI avant de déposer le nom de domaine. Le site de l'INPI (www.inpi.fr) informe sur les démarches à accomplir pour protéger une marque et sur les tarifs en vigueur, il permet en outre de télécharger le formulaire nécessaire.

- **Déclarer son site auprès de la CNIL (Commission Nationale Informatique et Libertés)**

Si le site collecte des informations nominatives, il faut informer les personnes concernées de l'existence et des modalités d'exercice du droit d'accès aux informations qui les concernent et du droit de les faire modifier (changement de nom, d'adresse, etc.), rectifier en cas d'erreur ou supprimer (Loi Informatique et Libertés).

Si des procédés particuliers sont mis en oeuvre pour collecter des données nominatives sans intervention des personnes concernées (cookies ou applets java), l'éditeur du site est tenu d'informer les visiteurs de l'objet de cette collecte et de la possibilité de s'y opposer.

Si le site procède à un traitement de données à caractère personnel (comme la collecte d'adresses électroniques), il faut le déclarer auprès de la CNIL.

Pour en savoir plus, consultez le site de la CNIL :

www.cnil.fr



CREER UN SITE WEB OU UN BLOG

• **Afficher les informations légales (mentions légales obligatoires)**

Identification de l'éditeur du site : La loi du 21 juin 2004 pour la confiance dans l'économie numérique fait obligation aux personnes qui éditent un site internet de tenir à la disposition du public, sur leur propre site, un certain nombre d'informations.

1) Dans le cas d'un site Internet édité par une personne morale, la page « mentions légales » du site doit contenir au moins :

- La raison sociale
- Le siège social
- Un numéro de téléphone
- Le nom du directeur de la publication / du responsable de la rédaction
- et s'il y a lieu, le capital social et le numéro d'inscription au registre du commerce et des sociétés (RCS).

2) Dans le cas d'un site Internet édité par une personne physique, La page « mentions légales » du site doit contenir au moins :

- Nom et Prénoms
- Adresse du domicile
- Numéro de téléphone
- et, le cas échéant, le numéro d'inscription au registre du commerce et des sociétés (RCS) ou au répertoire des métiers.

«Il est néanmoins possible de garder son anonymat, dès lors que les coordonnées exactes de l'éditeur ont été transmises de façon correcte à l'hébergeur.

C'est alors l'hébergeur qui sera tenu de communiquer les informations sur l'éditeur, mais uniquement dans le cadre d'une procédure judiciaire.»

Dans le cas d'une boutique de vente en ligne (site e-commerce), par exemple, les mentions spéciales suivantes doivent figurer sur le site :

- Les conditions générales de vente
- Le délai moyen de livraison
- Les conditions de remboursement

3) Dans tous les cas, les conditions d'hébergement doivent être clairement indiquées :

- Nom de l'hébergeur
- Raison sociale
- Adresse
- Numéro de téléphone

Le défaut de mise à disposition du public de ces informations est passible de sanctions pénales.

• **Le contenu du site doit être en conformité avec la législation :**

1) la **Loi sur la liberté de la presse** s'oppose à la mise en ligne d'écrits, d'images ou de sons à caractère diffamatoire, raciste ou révisionniste.

2) le **Code pénal (protection des mineurs)** interdit la mise en ligne de tout message à caractère violent, pornographique ou portant gravement atteinte à la dignité humaine susceptible d'être vu ou perçu par un mineur.

3) le **Code la propriété intellectuelle** interdit la reproduction et la mise en ligne d'une œuvre protégée ou d'une marque sans l'accord de son auteur, de ses ayants droit ou de son titulaire.



Ainsi, avant de reproduire tout texte, photographie, illustration, musique ou vidéo, il faut identifier les titulaires des droits sur ces œuvres et leur demander une autorisation écrite pour la reproduction et la mise en ligne des œuvres sur le site.

Cela vaut aussi pour des œuvres provenant d'Internet (Tout ce que l'on trouve sur le Net n'est pas libre de droits!).

De même, il est illégal de mettre en ligne ou de télécharger des fichiers musicaux (MP3...) sans l'accord écrit de l'ayant droit.



**Tout savoir sur les licences
"Creative Commons" :**
<http://creativecommons.fr/>

• Protéger le contenu de son site

Pour protéger correctement des œuvres (dessins, musiques, photos, articles etc.), on peut à nouveau recourir aux services payants de l'**INPI** (une dizaine d'euros pour protéger votre œuvre pour une durée de 5 ans).

Il existe d'autres moyens de protection des œuvres en ligne, tel que le **tatouage numérique** (watermarking) permettant d'authentifier une œuvre et son propriétaire en y associant des permissions particulières (par exemple, une autorisation de reproduire ou d'utiliser l'œuvre pour un usage privé).

Pour en savoir plus, lire l'article sur le watermarking de Wikipédia à l'adresse suivante :

http://fr.wikipedia.org/wiki/Tatouage_numérique



Que sont les réseaux sociaux ?

Il s'agit de sites Internet sur lesquels on peut s'inscrire en créant un "**profil**", c'est à dire une sorte de carte d'identité virtuelle.

Les réseaux sociaux permettent d'échanger avec d'autres membres inscrits sur le même réseau (exemple : Facebook, MySpace ou LinkedIn).

On peut y échanger des messages (messagerie instantanée), des liens, des contenus (photos, vidéos, jeux).

On peut aussi ajouter des "**amis**" et enrichir sa liste de contacts.

Ces espaces de convivialité (virtuelle?) ne sont cependant pas sans danger et c'est bien pour cela l'accès à Facebook est interdit aux moins de 13 ans, même si dans la réalité, un pourcentage non négligeable de jeunes de moins de 13 ans y sont malgré tout inscrits (18% des moins de 13 ans selon une étude récente).

Extrait du règlement de Facebook

" ... Inscription et sécurité des comptes

Les utilisateurs de Facebook donnent leur vrai nom et de vraies informations les concernant, et nous vous demandons de nous aider à ce que cela ne change pas. Voilà quelques conditions que vous vous engagez à respecter pour l'inscription et la sécurité de votre compte :

... (article) 5. Vous n'utiliserez pas Facebook si vous avez moins de 13 ans ... "

VEUX-TU ÊTRE MON AMI ? ... LES RÉSEAUX SOCIAUX

Les problèmes liés à l'utilisation des réseaux sociaux par les jeunes (enfants et adolescents) sont multiples :

- **Comportements addictifs :** Fréquence et durée des connexions)

- **Mise en ligne d'informations relevant de la sphère privées** (identité réelle, adresse postale, téléphone, photos ...)

- **Acceptation de nouveaux contacts concernant des personnes inconnues dans la vraie vie** (Les amis de mes amis ... ne sont pas toujours mes amis, surtout sur Internet!)

- **Comportements répréhensibles :** De même que dans la vie de tous les jours, tout n'est pas permis, et ceux qui se livrent à l'injure, à la diffamation ou au harcèlement tombent sous le coup de la loi.

Pour les jeunes mineurs, leurs parents sont responsables pénalement jusqu'à leur majorité.

- **Exposition à des insultes, mensonges et rumeurs, ou à des contenus choquants**, à caractère sexuel, violent, raciste ou homophobe ...

Face à ces problématiques, parents, enseignants et éducateurs sont parfois démunis et quelques conseils relevant du sens commun s'imposent :

- **Rappelez les règles des réseaux** (exemple : Facebook interdit aux moins de 13 ans) **et la législation en vigueur sur les réseaux sociaux comme dans la vraie vie** (souvenez vous qu'aux yeux de la loi, les parents sont les responsables légaux des enfants mineurs).

De même qu'il est très déplaisant d'être soi-même victime de rumeurs ou de calomnies, on peut comprendre que se livrer soi-même à l'injure ou la diffamation peut être nuisible à autrui et passible de poursuites en justice.

- **Informez vous régulièrement sur les nouvelles technologies pour ne pas être dépassé par les événements et engagez un dialogue avec le jeune** pour lui faire prendre conscience des risques relatifs à la divulgation d'informations privées liées à son intimité.

- **Avoir beaucoup d'amis** est peut être un critère de valorisation mais ne vaut-il pas mieux en avoir peu, mais qu'ils soient de vrais amis sur lesquels on peut compter dans la vraie vie.

Trois sites pour s'informer !

www.unaf.fr

Site de l'Union Nationale des Associations Familiales

www.jeunes.cnil.fr

Site de la CNIL dédié aux jeunes : Informations, didacticiels et fiches pratiques destinés aussi bien aux enfants et aux adolescents, qu'aux parents et aux enseignants.

www.actioninnocence.org

Site de Action Innocence : Une association de protection des enfants sur Internet : guides, affiches, dossiers ...

