Attitude citoyenne & TIC

Objectif : Adopter une attitude citoyenne dans l'utilisation des technologies de l'information et de la communication

Christine DEROIN – Octobre 2012

1 Les règles propres à l'usage des réseaux et de l'Internet

La nétiquette

Dans le passé, la population des gens qui utilisaient l'Internet avaient "grandi" avec l'Internet, étaient techniquement attentifs et comprenaient la nature des échanges et des protocoles. Aujourd'hui, la communauté des utilisateurs de l'Internet compte des gens qui sont nouveaux dans cet environnement.

Afin d'amener rapidement ces nouveaux utilisateurs à la culture de l'Internet, il existe un ensemble de règles de bonne conduite sur Internet, regroupées sous le nom de **nétiquette**.

Les règles de courtoisie

En général, les règles de courtoisie habituelle dans les rapports entre les gens devraient être de mise en toute circonstance et sur l'Internet, c'est doublement important là où, par exemple, l'expression corporelle et le ton de la voix doivent être déduits.

- ☺ Les messages ne doivent pas être injurieux ou haineux (on les appelle des "flammes") même si on vous provoque. D'autre part, il est prudent de ne pas répondre aux flammes.
- ☺ Les messages doivent être lisibles et clair avec une ponctuation appropriée
- ☺ Les messages doivent être signés. Rendez les choses faciles pour le destinataire. Certains relais de courrier enlèvent l'information d'en-tête qui reprend votre adresse d'expéditeur. Pour être sûr que les gens sachent qui vous êtes, veillez à mettre une ligne ou deux à la fin de votre message avec vos coordonnées. Vous pouvez créer ce fichier à l'avance et l'ajouter à la fin de vos messages. (Certains programmes de courrier font cela automatiquement.) En langage Internet, cela s'appelle un fichier .sig ou "signature". Votre fichier .sig remplace votre carte de visite. (Et vous pouvez en avoir plusieurs pour diverses circonstances.)
- ☺ Les formules de politesse (simplifiées par rapport à un courrier) sont souhaitées et les smiley ☺ bienvenus
- ☺ L'usage de la majuscule doit être limité car cela signifie que l'on crie
- ☺ Les messages auront toujours un objet (ou Subject) qui se rapporte au contenu.

Les règles techniques

- ☺ Les fichiers volumineux ne doivent pas être envoyés
- ☺ Le destinataire d'un message doit vérifier si le message qui lui est envoyé fait partie d'une liste, est une copie, un transfert ou un envoi personnel

Les règles de communauté

- ☺ les envois de lettre-chaîne sont à éviter
- ☺ de grandes quantités d'informations non demandées ne doivent pas être envoyées
- ☺ Si vous utilisez le courrier électronique sur votre lieu de travail, y compris pour traiter votre courrier personnel, veillez à vérifier avec votre employeur ce qu'il en est concernant la propriété du courrier électronique. Les règles concernant la propriété du courrier électronique diffèrent d'un endroit à l'autre.

Les règles de bon sens

- ☺ Les personnes s'expriment pour elles-mêmes et ce qu'elles expriment ne représente pas leur institution (sauf mention explicite)
- ☺ L'authenticité d'un message doit être vérifiée. Tout comme le courrier peut (aujourd'hui) n'être pas secret, le courrier sont sujets (aujourd'hui) à falsification et imposture, à des degrés divers de détection. Faites jouer votre bon sens et votre sens de la réalité avant de considérer un message comme authentique.
- ☺ Sauf en cas de cryptage, aucune information confidentielle ne doit circuler par courrier électronique. Ne mettez jamais dans un message électronique quelque chose que vous ne mettriez pas sur une carte postale.

1.1 Les chartes informatiques

Une charte informatique (appelée également charte Internet) est un document définissant les règles concernant tous les usages liés à Internet au sein d'une entreprise, d'une administration ou d'une association : navigation, courrier électronique, intranet, etc. Il recense les droits et obligations des salariés, des visiteurs, des stagiaires, tout en soulignant leurs responsabilités. Sa mise en place permet d'éviter toute forme d'abus dans l'usage des outils informatiques et fournit une référence en cas de conflit.

La charte de l'entreprise est considérée comme une adjonction au Règlement intérieur.

Sa rédaction est guidée par la préservation :

- ✓ des droits légitimes de l'employeur en matière de confidentialité, de sécurité et d'efficacité de ses systèmes d'informations ;
- ✓ du droit au respect de la vie du salarié et ce, en encadrant les conditions d'exploitation du système informatique, les modalités de contrôle de ceux-ci et les conséquences des manquements.

Exemple : Au Greta, il existe une charte informatique générale intégrée au livret stagiaire et une charte spécifique aux salles du bâtiment 6 consultable par affichage.

2 Les dangers liés aux réseaux et aux échanges de données

2.1 Les dangers

2.1.1 Spam ou pourriels

On entend par pourriels tous les messages non sollicités, publicitaires ou non, qui envahissent de plus en plus nos boîtes à lettres électroniques. Ce fléau s'est développé de manière spectaculaire et on estime qu'il représente désormais près de la moitié de tous les courriels.

Certains logiciels de messagerie permettent de s'en prémunir (courriers indésirables). Vous pouvez également vous créer une adresse électronique spéciale à communiquer aux sites marchands afin de limiter le nombre de spam dans votre boîte à lettres principale. Soyez également vigilant lorsque vous remplissez un formulaire en ligne. Vous avez la possibilité d'accepter ou non la communication de vos informations personnelles à des tiers et l'envoi de Newsletters. Enfin, vous pouvez toujours vous désabonner et signaler que vous ne voulez plus recevoir de messages.

2.1.2 Jeux de hasard

La prolifération des jeux de hasard et des sites de paris sur Internet n'a fait qu'augmenter le nombre impressionnant de personnes qui s'adonnent au jeu. Les jeunes qui maîtrisent bien les nouvelles technologies se tournent de plus en plus vers les sites Internet de jeux de hasard parce qu'ils sont faciles d'accès, pratiques et anonymes. C'est devenu chez les adolescents une addiction plus importante que la cigarette, l'alcool ou les drogues.

2.1.3 Désinformation

La Toile véhicule une quantité d'informations douteuses et sans valeur. Dans la mesure où n'importe qui peut facilement y diffuser ses théories ou opinions personnelles, les internautes doivent absolument acquérir une pensée critique qui les incite à vérifier la crédibilité de l'information trouvée en ligne.

La désinformation y est courante sous de multiples aspects :

- ✓ les sites haineux qui propagent des propos diffamatoires en diffusant ouvertement des points de vue extrémistes
- ✓ les sites commerciaux où les publicitaires créent des environnements à la fois informatifs et amusants dans le seul but de promouvoir leurs produits auprès d'un public cible
- ✓ les pages Web, généralement personnelles, où n'importe qui peut publier ce qu'il veut en prétendant que c'est vrai et présenter de simples opinions comme des faits
- ✓ les sites « pastiches » ou parodiques, qui induisent volontairement le visiteur en erreur, soit pour s'amuser, soit pour des raisons politiques, ou pour montrer aux jeunes combien il est facile de duper les gens en ligne
- ✓ les canulars diffusés par courriel, qui diffusent fausses alertes aux virus informatiques, procédés bidon pour soi-disant faire fortune, légendes urbaines et alarmes sanitaires infondées.

Comment vérifier la validité de l'information ?

- ✓ **Le repérage d'éléments fiables**

Plusieurs éléments peuvent être repérés afin de valider des informations ou tout au moins de les crédibiliser :

- Des informations sur l'auteur : son nom, son adresse, ses références (privilégiez toujours les sites officiels)
- Des informations sur le texte : des sources, sa date de création
- Une bibliographie
- Des liens vers d'autres documents qui abordent le même thème
- Des références (citations, nom d'ouvrages, d'auteurs…)

Afin de vérifier la véracité des informations, vous pouvez également les comparer à d'autres documents traitant du même sujet ou vous documenter pour connaître préalablement le sujet.

N'oubliez pas de faire marcher votre bon sens afin de vérifier la cohérence et la vraisemblance des informations que vous lisez !

✓ La vérification sur un site spécialisé dans la chasse aux canulars

Des milliers d'e-mails relatant de fausses informations circulent sur le réseau. La plupart du temps alarmants, ces messages ne sont en fait que des hoax (canulars). Fausses alertes aux virus, fausses chaînes de solidarité, fausses promesses, fausses informations, les hoax prennent toutes les formes

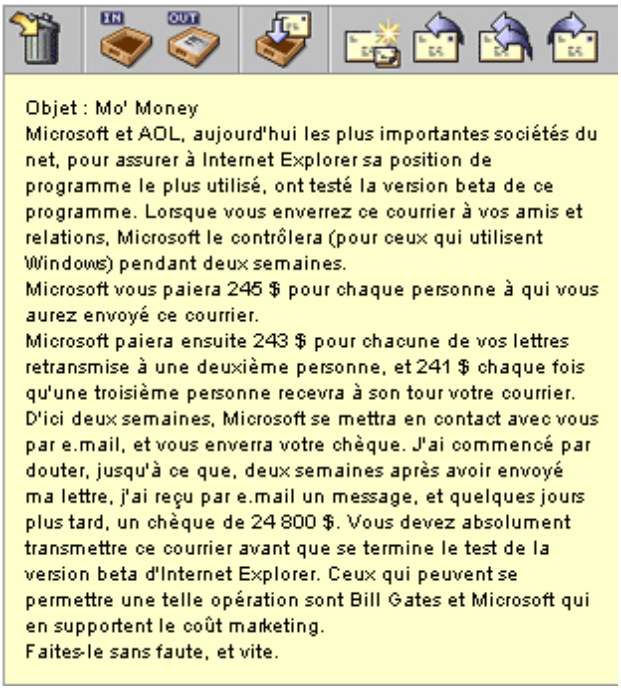
Lorsque vous recevez un courrier électronique envoyé par un ami vous alertant d'un nouveau type de virus, votre premier réflexe est de relayer cette alerte et donc de renvoyer au plus vite le message à toutes vos connaissances, qui feront à leur tour exactement la même chose et ainsi de suite jusqu'à ce que le message fasse plusieurs fois le tour du monde.

Changez vos habitudes : vérifiez avant de relayer !

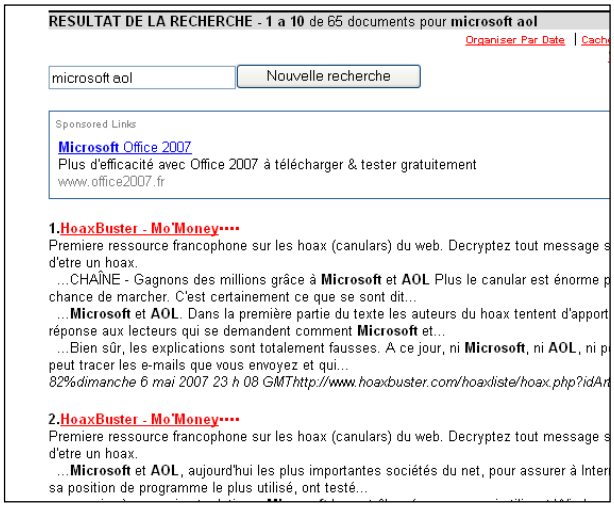
Un site Internet est devenu spécialiste dans la traque aux hoax. Je vous le recommande : **http://www.hoaxbuster.com**

Exemple :

- Vous recevez le message ci-contre :
- Rendez-vous sur site de hoaxbuster et dans la zone **Rechercher**, saisissez un ou plusieurs mots significatifs du message et cliquez sur **Go** :



- En quelques secondes Hoaxbuster affiche plusieurs liens vers des articles publiés sur le site. Le premier lien est souvent le bon et vous donnera l'information que vous recherchez. Cliquez sur ce lien :

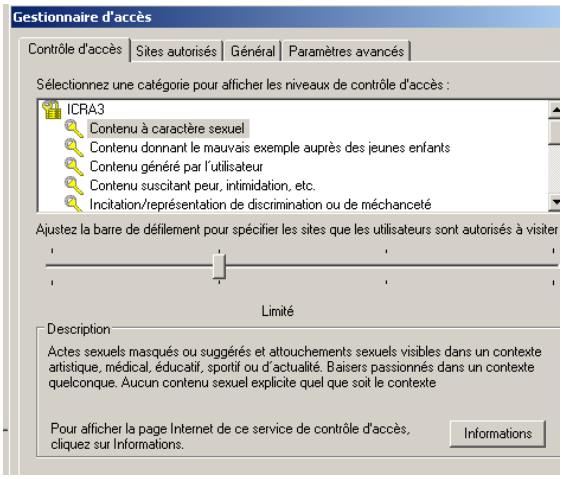


- Hoaxbuster vous donne des informations fiables sur le message en le classifiant par type (rumeur, chaîne, désinformation, solidarité, etc....) par statut (voir légende ci-contre) et par date de mise en circulation.

2.1.1 Une cible facile : les enfants

Internet est un moyen d'accès sans précédent à un large éventail d'informations. Cependant, certaines informations peuvent ne pas être adaptées à tous les utilisateurs. Par exemple, vous pouvez estimer que vos enfants ne doivent pas avoir accès au contenu de sites Web à caractère violent ou sexuel.

Le navigateur Internet Explorer permet de filtrer l'accès aux informations dans le cadre d'un contrôle parental par le biais du **Gestionnaire d'accès**. Il permet de contrôler les types de contenu auxquels votre ordinateur peut accéder sur Internet. Une fois le contrôle d'accès activé, seul le contenu correspondant à vos critères peut être affiché. Vous pouvez moduler les paramètres (niveaux) pour chacune des catégories proposées.



Le Gestionnaire d'accès est accessible en choisissant les rubriques suivantes :

- **Sécurité**
- **Déclaration de confidentialité de la page Web**
- **Paramètres**
- Onglet **Contenu**

2.1.2 Pistage et traces

Sur internet comme ailleurs, vos activités et vos déplacements laissent des traces. L'impression de facilité qui domine l'univers de la Toile masque la réalité d'une surveillance discrète et active.

Le pistage par la reconnaissance de la configuration de votre ordinateur :

Chaque site auquel vous vous connectez connaît notamment :

- ✓ votre adresse IP,
- ✓ votre nom d'hôte qui lui-même révèle le nom de votre fournisseur d'accès,
- ✓ votre système d'exploitation,
- ✓ la page qui vous a conduit jusqu'à lui

Le pistage par les cookies

Un cookie est un fichier stocké sur le disque dur de l'utilisateur, afin de permettre au serveur web de le reconnaître d'une page web à l'autre. Les cookies sont notamment utilisés par les sites de commerce électronique afin de conserver les préférences de l'utilisateur (par exemple les options qu'il a coché) afin de lui éviter de les ressaisir.

Le problème majeur des cookies relève des informations qu'ils contiennent. En effet, lorsqu'un utilisateur se connecte à un site personnalisable, celui-ci va lui poser quelques questions afin de dresser son profil, puis stocker ces données dans un cookie. Selon le site, la manière de laquelle l'information est stockée peut s'avérer nuisible à l'utilisateur.

En effet, un site de vente en ligne peut par exemple collecter des informations sur les préférences des utilisateurs par le biais d'un questionnaire, afin de leur proposer ultérieurement des articles pouvant les intéresser.

Par exemple, en sachant si l'utilisateur est un homme ou une femme, un site pourra l'aiguiller directement au rayon approprié pour lui faire économiser du temps (et surtout pour mieux vendre). Si par ailleurs, l'utilisateur a indiqué dans son profil qu'il est amateur de tennis, le site sera en mesure de lui proposer une sélection personnalisée des derniers articles en la matière.

Un cookie est ainsi un mécanisme prévu pour créer une association entre la session de l'utilisateur (navigation entre des pages d'un même site pendant une période donnée) et les données le concernant.

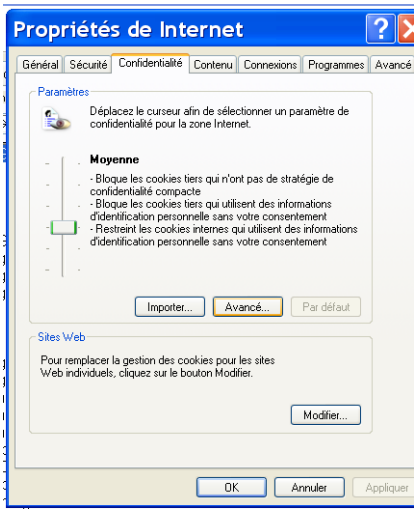
Comment se protéger ?

Un cookie n'a rien de dangereux en soi s'il est bien conçu et si l'utilisateur ne donne pas d'informations personnelles.

Ainsi, refusez de céder des informations personnelles à un site ne vous inspirant pas confiance car il n'a aucune raison de collecter des informations vous concernant.

Vous pouvez également régler votre navigateur pour optimiser votre protection.

Les fonctionnalités de confidentialité vous permettent de protéger vos informations identifiables personnellement, en vous aidant à comprendre comment les sites Web que vous consultez utilisent ces informations et en vous permettant de spécifier des paramètres de confidentialité déterminant si vous souhaitez ou non autoriser les sites Web à enregistrer les cookies sur votre ordinateur.



Pour paramétrer le degré de confidentialité :

- ✓ Dans Internet Explorer, choisir **Sécurité** :
- ✓ **Déclaration de confidentialité de la page Web**
- ✓ **Paramètres**
- ✓ Onglet **Confidentialité**
- ✓ Déplacer le curseur sur « **Moyenne** »
- ✓ Valider par **OK**

2.1.3 Hameçonnage (phishing)

Le hameçonnage, ou phishing, est une technique frauduleuse utilisée pour obtenir des renseignements personnels auprès d'internautes. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc.

La technique du phishing est une technique d'ingénierie-sociale, c'est-à-dire consistant à exploiter non pas une faille informatique mais la « faille humaine » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce.

Comment se protéger du phishing ?

Lorsque vous recevez un message provenant a priori d'un établissement bancaire ou d'un site de commerce électronique il est nécessaire de vous poser les questions suivantes :

- Ai-je communiqué à cet établissement mon adresse de messagerie ?
- Le courrier reçu possède-t-il des éléments personnalisés permettant d'identifier sa véracité (numéro de client, nom de l'agence, etc.) ?

Par ailleurs il est conseillé de suivre les conseils suivants :

- Ne cliquez pas directement sur le lien contenu dans le mail, mais ouvrez votre navigateur et saisissez vous-même l'URL d'accès au service.
- Méfiez-vous des formulaires demandant des informations bancaires. Il est en effet rare (voire impossible) qu'une banque vous demande des renseignements aussi importants par un simple courrier électronique. Dans le doute contactez directement votre agence par téléphone !
- Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par https et qu'un petit cadenas est affiché dans la barre d'état au bas de votre navigateur, et que le domaine du site dans l'adresse correspond bien à celui annoncé (gare à l'orthographe du domaine) !

2.2 Les risques techniques

2.2.1 Les virus

Un virus informatique est un programme qui modifie à votre insu le comportement de votre ordinateur.

Le nombre de virus connus et/ou en circulation est difficilement indentifiable et sujet à controverse selon les sources (journalistiques ou développeurs d'anti-virus).

Comportement du virus :

Il se propage et s'auto duplique d'un fichier à l'autre

Il active des symptômes ou dommages prévus par le réalisateur du virus notamment dans la plupart des cas, la modification ou la destruction de fichiers, le ralentissement d'exécution, voire même l'effacement du disque dur ou encore des effets visuels ou sonores surprenants...

Les différents modes de contamination :

Les virus infectent les fichiers en s'attachant aux programmes effectuant une action directe ou indirecte.

Les virus système (ou virus d'amorçage) s'attaquent au boot-sector ou aux répertoires ; ce qui peut engendrer la destruction de votre disque dur. Si vous n'avez pas effectué de sauvegarde au préalable, l'ensemble de vos données sera perdu.

Les macros virus affectent les commandes d'une application, notamment les fichiers modèles utilisés pour la création des documents. Ainsi lors de la création d'un nouveau document, le virus s'exécutera.

Un virus peut être transmis par un support amovible (clé USB, disque dur externe) ou par Internet (ouverture d'un fichier attaché d'un courriel, téléchargement d'un utilitaire).

Les différentes familles de virus :

LE VER ou WORM : Le ver est un virus qui a la capacité de s'auto reproduire et de se déplacer de manière totalement autonome dans un réseau.

LE CHEVAL DE TROIE OU TROJAN : Ils se présentent la plupart du temps sous la forme de programmes de types utilitaires ou jeux. C'est donc notamment lors d'un téléchargement de logiciels que le risque est plus grand; mais aussi via le fichier attaché d'un émail.

Il récupère les mots de passe d'un ordinateur, détruit les fichiers et prend le contrôle total de votre ordinateur dès qu'il est connecté à un Internet.

LES MACRO-VIRUS : Développés à partir du langage VisualBasic, langage communément utilisé pour la création de macros commandes depuis Office, les macros virus se développent rapidement. Ils s'intègrent à l'environnement global du logiciel souvent par le biais du fichier modèle NORMAL.DOT.

Une précaution à prendre : vérifier le niveau de sécurité dans vos logiciels de navigation et de messagerie.

La détection des virus :

Le premier principe d'un virus est de ne pas se faire repérer.

Symptômes :

- Un fichier infesté pourra changer de taille, de date de création, etc…
- La mémoire disponible sera moindre que celle constatée habituellement
- Le fonctionnement inhabituel de votre ordinateur : ralentissement de l'exécution des programmes, aspect de l'écran modifié, etc…

Toutefois, ces symptômes ne sont parfois pas assez significatifs pour vous alerter.

La protection contre les virus :

- Se munir d'un anti-virus (voir liste ci-dessous) : ces programmes détectent les virus d'après une collection de signatures.
- Effectuer des mises à jour périodiques de l'anti-virus (appelées couramment Update). : l'efficacité d'un anti-virus dépendra de la fréquence (une fois par semaine) de cette mise à jour
- Contrôler à l'aide d'un anti-virus les fichiers téléchargés ou en provenance d'une clé USB, d'un disque dur externe ou d'un cd-rom (risque moindre)
- Ne pas ouvrir un fichier attaché d'un courriel si vous ne connaissez pas l'émetteur.

- Ne pas ouvrir un fichier attaché d'un courriel accompagné des extensions suivantes : VBS, .VBE, .JS, .JSE, .HTA, .WSF, .WSH, .SHS, .SHB ou .EXE, CAM, .BAT, .SCR
- Ne pas ouvrir un fichier attaché d'un courriel accompagné d'une double extension : derrière une extension anodine telle que txt (format texte), jpg (format image), avi (format vidéo) peut se trouver une deuxième extension vbs ou exe par exemple (Ex: fichier.jpg.exe).
- Effectuer régulièrement des sauvegardes de vos fichiers de travail sur un support indépendant de votre disque dur.

La composition d'un anti-virus :

La plupart des anti-virus sont composés des modules suivants :

- Scanner : programme qui explore les fichiers à la recherche de virus connus. Les virus connus sont consignés dans une base de signature, que vous devez mettre à jour régulièrement.
- Temps réel : Scanner permanent en mémoire qui inspecte les fichiers dès qu'ils sont utilisés.
- Planificateur de tâches : Permet d'automatiser les analyses, mises à jour à un jour et une heure précise.
- Moniteur d'activité : Surveille en permanence l'activité de votre ordinateur et prévient l'utilisateur en cas de phénomènes suspects.
- Vérificateur d'intégrité : Stocke une base de données (du contenu d'un ordinateur), en effectuant régulièrement des comparaisons de l'état de votre ordinateur à cette même base ; il peut détecter des changements dus à des virus.

L'éradication des virus :

- Passer l'ensemble de vos unités de stockage à l'anti-virus (qui sera à jour des nouvelles bases virus)
- Laisser l'anti-virus réparer les fichiers contaminés ou les supprimer, si nécessaire
- Effectuer une nouvelle vérification de votre système à l'aide de l'anti-virus, à ce stade le logiciel devrait avoir supprimé le virus.
- Dans la négative, contacter un spécialiste.

Les liens utiles :

Antivirus gratuits :

http://www.avast.com/eng/download-avast-home.html (Avast Anti-virus)
http://www.free-av.com/antivirus/allinonen.html (AntiVir)
http://www.grisoft.com (AVG Free Edition)

Antivirus payants :

http://www.kaspersky.com/fr (Kapersky Lab)
http://www.bitdefender.fr (Bit Defender)
http://eset.entelechargement.com (Nod 32)
http://www.mcafee.com/ (VirusScan)
http://www.symantec.com/ (NortonAntiVirus)

Attention, **il ne faut pas utiliser plusieurs antivirus simultanément**. Ils risquent de se perturber, voire d'entraîner des dysfonctionnements et de ralentir le système, chacun d'eux pouvant croire que l'autre contient des virus !

2.2.2 Les intrusions

Lorsqu'il y a connexion à Internet, des informations entrent et sortent de votre ordinateur. Pour cet échange, on utilise une « porte », appelée port (il peut y en avoir plusieurs). Des pirates utilisent certains programmes conçus pour rechercher sur Internet toutes les personnes qui laissent leurs « ports » ouverts afin de s'introduire dans leur ordinateur et s'emparer de leurs fichiers.

La protection contre les intrusions :

- Votre mot de passe ne doit pas être trop simple (ex: nom de l'utilisateur, initiales etc..)
- Ne communiquez jamais votre mot de passe ou login : il vous est personnel et doit rester confidentiel.
- Ne laissez pas d'informations confidentielles sur votre ordinateur comme un numéro de carte bancaire
- Procurez-vous également un pare-feu ou FireWall (voir liste plus bas)

La protection par un pare-feu ou FireWall :

En effet, la meilleure parade contre les pirates est le pare-feu :

- Installé sur votre ordinateur, il permet de filtrer les communications et de se protéger contre les attaques réseaux.
- Son action se situe au niveau des ports de votre ordinateur, il filtre, ouvre ou ferme ceux-ci.
- Il identifie de façon systématique les pirates et bloque les tentatives d'accès
- Il rend automatiquement votre ordinateur invisible à tous les internautes

Le Pare-feu examine tout le trafic réseau qui arrive sur votre ordinateur et pose les questions suivantes :

- De quelle zone provenait le trafic et à quel port est-il adressé ?
- Les règles de cette zone autorisent-elles le trafic via ce port ?
- Ce trafic viole-t-il des règles globales ?
- Le trafic est-il autorisé par un programme de votre ordinateur (paramètres de contrôle des programmes) ?

Les réponses à ces questions déterminent si le trafic doit être bloqué ou autorisé.

Les liens utiles :

Pare-feu gratuits :

http://www.zonelabs.com/store/content/home (ZoneAlarme)

http://www.comodo.com (Comodo Firewall)

http://www.commentcamarche.net/download/telecharger-198-jetico-personal-firewall (Jetico Personal Firewall)

Pare-feu payants :

http://www.zonelabs.com/store/content/home (ZoneAlarme Pro)

http://www.symantec.com/ (Norton Personal FireWall)

http://www.mcafee.com/ (McAfee FireWall)

3 Les droits et obligations définis par la loi Informatique et Libertés

En France, la loi « Informatique et Libertés » réglemente l'utilisation des fichiers informatiques. Elle veille à ce que l'informatique ne porte pas atteinte « à l'identité humaine, aux droits de l'homme, à la vie privée, aux libertés individuelles ou publiques ».

Cette loi, votée le 6 janvier 1978 en France, a été modifiée à plusieurs reprises par plusieurs autres textes de loi et renforcée le 6 août 2004. Elle **protège surtout la vie privée et les informations nominatives**. Une information nominative est une information qui permet directement ou indirectement **l'identification d'une personne** (exemple : un n° de sécurité sociale, un nom, une adresse, etc…).

3.1 Les droits relatifs à la protection de la vie privée et des informations nominatives

La loi « Informatique et Libertés » reconnaît aux personnes vivant en France **4 droits fondamentaux** sur les informations les concernant :

1. Le droit à l'information
2. le droit d'opposition
3. le droit d'accès
4. le droit de rectification

Ces droits constituent les **limites à l'utilisation des fichiers informatiques**. Le non-respect de ces droits est sanctionné pénalement.

3.1.1 Le droit à l'information

Toute personne a le droit de savoir si elle est fichée et dans quels fichiers elle est recensée. Ce droit de regard sur ses propres données personnelles vise aussi bien la collecte des informations que leur utilisation. Toute personne qui met en œuvre un fichier ou un traitement contenant des données personnelles doit informer les personnes fichées de :

- l'identité du responsable du traitement,
- l'objectif de la collecte d'informations,
- le caractère obligatoire ou facultatif des réponses,
- les conséquences de l'absence de réponse,
- les destinataires des informations,
- les droits reconnus à la personne,
- les éventuels transferts de données vers un pays hors de l'Union Européenne.
- Dans le cadre d'une utilisation de réseaux, les personnes doivent être informées de l'emploi éventuel de témoins de connexion (cookies, variables de session …), et de la récupération d'informations sur la configuration de leurs ordinateurs (systèmes d'exploitation, navigateurs…).

Les limites au droit à l'information

Il est des cas où l'obligation d'information est allégée :

- lorsque les données collectées sont très vite anonymisées,
- lorsque les données ne sont pas recueillies directement auprès de la personne.

Il est des cas où l'obligation d'information est exclue :

- pour les fichiers de police ou de gendarmerie,
- pour les fichiers relatifs à des condamnations pénales,
- lorsque l'information de la personne se révèle impossible ou très difficile.

En pratique : Dans la mesure du possible, les personnes sont informées au moment de la collecte de leurs données. Les questionnaires doivent mentionner l'identité du responsable du fichier, l'objectif de la collecte d'informations, le caractère obligatoire ou facultatif des réponses fournies et les droits reconnus à la personne. Dans le cas d'un fichier constitué à l'aide de données cédées, louées ou achetées, l'information des personnes concernées doit être réalisée dès la création du nouveau fichier. S'il est prévu que les données soient transmises à d'autres personnes, l'information doit être réalisée au plus tard lors de la première communication des données.

3.1.2 Le droit d'opposition

Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier.

Toute personne peut refuser, sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection, en particulier commerciales.

En principe, toute personne peut décider elle-même de l'utilisation de données la concernant. En ce sens, elle peut refuser d'apparaître dans certains fichiers ou de voir communiquer des informations sur elles à des tiers.

Le droit d'opposition peut s'exprimer :

- par un refus de répondre lors d'une collecte non obligatoire de données,
- par le refus de donner l'accord écrit obligatoire pour le traitement de données sensibles telles que les opinions politiques ou les convictions religieuses,
- la faculté de demander la radiation des données contenues dans des fichiers commerciaux,
- la possibilité d'exiger la non-cession ou la non-commercialisation d'informations, notamment par le biais d'une case à cocher dans les formulaires de collecte ...

Les limites au droit d'opposition

Le droit d'opposition n'existe pas pour de nombreux fichiers du secteur public comme, par exemple, ceux des services fiscaux, des services de police, des services de la justice, de la sécurité sociale … .

En pratique :

Le droit d'opposition s'exerce au moment de la collecte d'informations ou plus tard en s'adressant au responsable du fichier.

Le droit d'opposition ne doit occasionner aucun frais à la personne qui l'exerce.

3.1.3 Le droit d'accès

(Articles 39, 41, 42 de la loi du 6 janvier 1978 modifiée)

Toute personne justifiant de son identité a le droit d'interroger le responsable d'un fichier ou d'un traitement pour savoir s'il détient des informations sur elle, et le cas échéant d'en obtenir communication.

Toute personne peut prendre connaissance de l'intégralité des données la concernant et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.

En exerçant son droit d'accès, la personne peut s'informer des finalités du traitement, du type de données enregistrées, de l'origine et des destinataires des données, des éventuels transferts de ces informations vers des pays n'appartenant pas à l'Union Européenne.

Toute personne est en droit d'obtenir des explications sur le procédé informatique qui a contribué à produire une décision la concernant.

L'exercice du droit d'accès permet de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer. Le juge des référés peut être saisi en cas de risque de dissimulation ou de disparition des données.

Les limites au droit d'accès

Si un responsable de traitement estime qu'une demande est manifestement abusive, il peut ne pas y donner suite. En revanche si l'affaire est portée devant un juge il devra apporter la preuve du caractère manifestement abusif de la demande en cause.

Le droit d'accès ne s'exerce pas lorsque les données sont conservées sous une forme ne présentant aucun risque d'atteinte à la vie privée et pendant une durée n'excédant pas celle nécessaire à l'établissement de statistiques ou à la recherche scientifique ou historique.

L'exercice du droit d'accès ne doit pas porter atteinte au droit d'auteur.

En pratique : Le droit d'accès s'exerce directement auprès de l'organisme qui détient des informations.

La communication des données doit être fidèle au contenu de ce qui est enregistré dans l'ordinateur et effectuée en langage clair.

À noter : Depuis 2002, une personne peut accéder directement à son dossier médical.

Régime particulier : le droit d'accès indirect

- Le droit d'accès aux fichiers de police et de gendarmerie (article 41)
- Le droit d'accès en matière d'infractions et d'imposition (article 42)

En principe, le droit d'accès aux fichiers de police et de gendarmerie ou à un traitement visant à prévenir, rechercher ou contrôler des infractions, ou encore à recouvrer des impositions s'exerce par l'intermédiaire d'un commissaire de la CNIL.

Ce commissaire, magistrat ou ancien magistrat, effectue les investigations utiles et fait procéder aux modifications nécessaires, par exemple la rectification ou l'effacement de données inexactes.

La CNIL notifie ensuite par courrier au demandeur qu'il a été procédé aux vérifications. Cette lettre indique la fin de la procédure administrative ainsi que les voies et délais de recours contentieux qui sont ouverts.

Toutefois, lorsque cela ne met pas en cause la sûreté de l'État, la défense ou la sécurité publique, les données peuvent être communiquées directement à la personne qui a souhaité exercer son droit d'accès.

3.1.4 Le droit de rectification

Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations qui la concernent lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Le droit de rectification constitue un complément essentiel du droit d'accès.

Lorsque des modifications sont apportées aux données concernant une personne qui a exercé son droit de rectification, le responsable du traitement doit justifier, sans frais pour la personne qui en a fait la demande, des opérations qu'il a effectuées.

À noter : Les héritiers d'une personne décédée peuvent exiger que le responsable d'un traitement comportant des données concernant le défunt prenne en considération le décès et procède aux mises à jour.

En pratique : Pour exercer son droit de rectification, il faut écrire à l'organisme qui détient les informations.

En retour, le responsable du traitement doit prouver qu'il a procédé aux rectifications demandées et les notifier aux tiers à qui auraient été transmises les données erronées.

Le demandeur peut obtenir gratuitement une copie de l'enregistrement modifié.

En cas de litige, le responsable du traitement doit apporter la preuve qu'il a donné suite à la demande de rectification

3.2 Les obligations des créateurs de fichiers nominatifs

Les créateurs de fichiers nominatifs ont des obligations à respecter

- Parce qu'un traitement de données personnelles n'est pas un fichier comme les autres
- Parce que ça concerne des parcelles de vie privée
- Parce que cela peut porter atteinte aux libertés.

Ils sont pénalement responsables, toujours au regard de la Loi Informatique et Libertés, de l'application des 7 **principes clefs** à respecter dans l'utilisation **des données personnelles**, en ce qui concerne :

- La collecte
- La finalité
- La conservation
- La sécurité
- La confidentialité
- L'information
- La déclaration

3.2.1 La collecte des données

En principe, il faut recueillir le consentement de la personne pour utiliser une information qui l'identifie.

Les données traitées doivent être exactes, complètes et mises à jour.

Sauf dérogations, on ne peut pas collecter des données sensibles (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, données relatives à la vie sexuelles ou à la santé).

3.2.2 La finalité

L'usage des données personnelles doit être déterminé et légitime, et ce dès la collecte des informations. Cet usage doit correspondre aux missions de l'administration et de chacun de ses services responsables du traitement.

Les informations recueillies doivent être pertinentes, adéquates et non excessives par rapport à la finalité du traitement.

Exemple : un fichier nominatif municipal ne peut être utilisé à des fins commerciales ou politiques.

3.2.3 La conservation

Les informations nominatives ne peuvent être conservée plus d'une certaine durée, déterminée avec les Archives de France. Au-delà de cette durée, les données nominatives doivent être détruites ou archivées si elles présentent un intérêt historique, statistique ou scientifique.

Exemple : le fichier d'une personne enregistrée au service d'aide sociale ne peut pas être conservé plus d'un an à compter de la dernière aide.

3.2.4 La sécurité des fichiers

Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux) et logiques (sécurité des systèmes d'information) adaptées à la nature des données et aux risques présentés par le traitement.

Exemple : l'accès aux informations nominatives doit être limité par un mot de passe.

3.2.5 La confidentialité

Les données personnelles ne peuvent être consultées que par les services concernés par ces informations. Elles ne peuvent être communiquées qu'exceptionnellement à des autorités (par exemple le Trésor Public) et selon une procédure particulière.

Exemple : un fichier cadastral ne peut être utilisé que par les services de l'urbanisme, du cadastre et de la voirie.

3.2.6 L'information

Le responsable d'un fichier doit permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits.

Pour cela, il doit leur communiquer son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits, les transmissions envisagées.

3.2.7 La déclaration

Certains traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en oeuvre, être déclarés ou soumis à la CNIL.

3.3 La CNIL : l'institution chargée de veiller au respect de la loi

Le sigle CNIL signifie **Commission Nationale de l'Informatique et des Libertés**.

Elle est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques

Cette autorité administrative indépendante est composée de 17 membres. Elle a pour mission de veiller au respect de la loi et d'informer les personnes sur leurs droits et leurs obligations.

La CNIL possède un **pouvoir de surveillance et de contrôle**. Elle lutte contre le **traçage de l'internaute**. Elle peut alors réprimer et porter devant les tribunaux ces abus.

La CNIL doit valider tout fichier informatique nominatif et ce avant sa création (elle vérifie si la loi est respectée et émet un avis).

Elle veille, en particulier, à ce qu'un créateur de fichier nominatif ait obtenu l'accord écrit de la personne pour faire figurer des informations dites « sensibles ». Les informations « sensibles » sont les données nominatives qui, directement ou indirectement, font apparaître :

- Les origines ethniques,
- les sensibilités politiques,
- les opinions philosophiques,
- les convictions religieuses,
- les appartenances syndicales,
- les mœurs des personnes.

La version du 6 août 2004 de la loi « Informatique et Libertés » a renforcé les pouvoirs d'intervention de la CNIL et accorde dans ce nouveau dispositif législatif une large place aux contrôles à posteriori. Elle simplifie les formalités déclaratives, le contrôle préalable de la CNIL étant désormais limité aux seuls traitements présentant des risques particuliers d'atteinte aux droits et libertés. Enfin, elle renforce les droits des personnes sur leurs données.

Pour en savoir plus sur la CNIL : http://www.cnil.fr

4 Le respect de la propriété intellectuelle

La propriété intellectuelle se présente sous deux aspects :

- la propriété industrielle
- la propriété littéraire et artistique

Par **propriété intellectuelle**, on entend donc les **créations de l'esprit** : les **inventions**, les **oeuvres littéraires** et **artistiques**, mais aussi les **symboles**, les **noms**, les **images** et les **dessins** et **modèles** dont il est fait usage dans le commerce.

La propriété intellectuelle est protégée par le **Code de la propriété intellectuelle**, texte de loi dont la dernière version consolidée date du 11 septembre 2011.

Avec l'outil informatique et la généralisation de l'Internet, les droits d'auteur sont mis à mal.

Qu'est-ce que le droit d'auteur ?

Le droit d'auteur désigne l'ensemble des droits dont jouissent les **créateurs** sur leurs **oeuvres littéraires et artistiques** (les romans, les poèmes et les pièces de théâtre, les films, les oeuvres musicales, les oeuvres d'art telles que dessins, peintures, photographies et sculptures, ainsi que les créations architecturales).

Les droits connexes du droit d'auteur sont les droits que possèdent les artistes interprètes ou exécutants sur leurs prestations, les producteurs d'enregistrements sonores sur leurs enregistrements, et les organismes de radiodiffusion sur leurs programmes radiodiffusés et télévisés.

Quelles sont les oeuvres protégées par le droit d'auteur ?

Les oeuvres protégées par le droit d'auteur comprennent notamment les oeuvres littéraires (romans, poèmes, pièces de théâtre, ouvrages de référence, journaux et logiciels), les bases de données, les films, compositions musicales et oeuvres chorégraphiques, les oeuvres artistiques telles que les peintures, dessins, photographies et sculptures, architecture, et les créations publicitaires, cartes géographiques et dessins techniques.

Les œuvres sont protégées dès que son auteur les déposent et jusqu'à 70 ans après son décès (entre son décès et la fin de la protection de l'œuvre, ce sont ses héritiers qui perçoivent les droits). Au-delà de ce temps, l'œuvre tombe dans le domaine public.

Quelques exemples :

Question : Suis-je dans l'illégalité si je vends des jeux vidéos gravés ? (4.5 € /jeu)

Réponse : OUI ! Le code de la propriété intellectuelle qualifie de contrefaçons la reproduction intégrale ou partielle d'une œuvre protégée faite sans le consentement de son auteur. Vous êtes un contrefacteur et vous risquez deux ans d'emprisonnement et 150 000 € d'amende.

Question : Je travaille avec mes élèves sur le son. Ils copient un extrait de 30 secondes d'un CD audio sur disque dur et y rajoutent leurs commentaires. Ai-je le droit de les insérer sur le site Internet de l'école ?

Réponse : Avant de diffuser sur le site Internet de votre école des extraits musicaux commentés de 30 secondes au moins, il est nécessaire que vous obteniez une autorisation préalable, écrite et expresse du titulaire des droits sur ces extraits. Vous pouvez vous adresser à la Sacem (Société des Auteurs, Compositeurs et Editeurs de Musique).

Plus d'informations :

Code de la propriété intellectuelle en France :
http://www.copyrightfrance.com/hypertext/cpi1.htm

La propriété littéraire et artistique :
http://www.culture.gouv.fr/culture/infos-pratiques/droits/

Le site de la Sacem :
http://www.sacem.fr

5 Le droit à l'image

Selon les articles 226-1 à 226-8 du Code civil, « tout individu jouit d'un droit au respect de sa vie privée ainsi que d'un droit à l'image ».

En vertu de ces dispositions, la publication ou la reproduction d'une photographie sur laquelle une personne est clairement reconnaissable n'est possible qu'avec son consentement préalable, que l'image soit préjudiciable ou non. Font exception à cette règle les photos de foule où la personne n'est pas le sujet central ou bien les photos prises de loin ou de dos.

Le consentement est obtenu par la signature d'un document par la ou les personnes concernées par la photographie. Ce document doit faire apparaître les mentions permettant de faire référence aux photos concernées par l'autorisation et à l'utilisation qui en est faite. Il ne peut en aucun cas être établie d'autorisation globale, couvrant tout type de photographie impliquant la personne.

Certains aménagements ont été opérés concernant les personnalités publiques, sans mettre à mal le principe de base.

Dans le cas des enfants mineurs, la signature d'autorisation des parents de l'enfant ou de ses tuteurs légaux doit également être obtenue par écrit.

6 La loi HADOPI 2

La loi française n° 2009-1311 relative à la protection pénale de la propriété littéraire et artistique sur internet est communément appelée "HADOPI 2 " en référence à la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet qui a été institué pour la faire respecter.

Cette loi, après différents recours auprès du Conseil Constitutionnel, a finalement été promulguée le 28 octobre 2009. Les décrets d'application ont été au Journal officiel de la République française le 31 décembre 2009.

La loi vise à enrayer le téléchargement illégal de musique et/ou de films. Pour ce faire, le texte institue un mécanisme de "riposte graduée ".

Lorsqu'un internaute télécharge illégalement une œuvre musicale ou cinématographique depuis Internet, il est rappelé à l'ordre, d'abord par l'envoi de courriel d'avertissement puis, en cas de récidive, d'une lettre recommandée, et enfin par la suspension, voire la résiliation de son abonnement Internet.

Sources documentaires

http://www.commentcamarche.net

http://www.journaldunet.com

http://client.olfeo.com

http://www.ac-toulouse.fr

http://www.interieur.gouv.fr

http://www.legifrance.gouv.fr

http://www.droit-image.fr

http://www.lexpress.fr