Formation informatique

IU1

Formation à l'usage de l'Internet

niveau de base

La toile et les communications privées et publiques

IU1 – Formation à l'usage de l'Internet – niveau de base

La toile et les communications privées et publiques

Table des matières

1 Notions d'informatique

1.1 Principes et définitions

Certains termes sont accompagnés de leur traduction en anglais ou d'une abréviation courante (entre parenthèses et en italique). Les noms de marques et de produits sont en italique.

Ordinateur (personal computer = PC)

> Machine composée d'éléments matériels (*hardware*) tels que des composants électroniques, capables d'effectuer des opérations de calcul et de logique, ainsi que des pièces mécaniques. Ces composants sont alimentés en énergie électrique.
>
> L'ordinateur dispose en général de périphériques d'entrée (exemples : clavier, souris, lecteur de disques) et de périphériques de sortie (exemple : moniteur (écran), haut-parleur), ainsi que de périphériques de stockage (exemple : mémoire vive, disque dur).

Programme informatique (computer program)

> Ensemble d'instructions codées, destinées à être exécutées par la machine, permettant d'effectuer certaines opérations.

Libre vs *propriétaire ; ouvert* vs *fermé*

> En informatique, est dit « libre » (*free software*) un programme qui peut être librement utilisé, étudié, copié et modifié puis rediffusé. Ces programmes produisent des données dans des formats ouverts, c'est à dire lisibles par tous. Les programmes libres sont presque tous gratuits. Les programmes libres sont produits le plus souvent par des fondations sans but lucratif ou par des groupes d'individus qui travaillent bénévolement. Le but est de donner aux utilisateurs la plus grande liberté. Il y a une tradition d'entraide parmi les utilisateurs.
>
> Les programmes propriétaires (on dit aussi « privateurs ») sont protégés par les sociétés commerciales qui les produisent de façon que l'on ne peut que les utiliser dans les conditions prévues par le producteur. Ces programmes produisent des données dans des formats fermés (ou « propriétaire »), c'est à dire qui ne peuvent être lus que par eux-mêmes ou en payant une taxe. Les programmes propriétaires peuvent être gratuits (*freeware*) ou payants. Les sociétés qui produisent ces programmes ont pour seul objectif de faire du profit. Elles cherchent le plus souvent à piéger les utilisateurs. Ces programmes et les données qu'ils produisent peuvent présenter divers dangers (présence de virus, vol de données personnelles, données non lisibles après quelques années, *etc*.).

Droit d'auteur et licence d'utilisation

> La plupart des programmes informatiques et des œuvres de création sont protégés par le droit d'auteur (*copyright*). Les programmes sont de plus accompagnés d'une licence (contrat juridique) que l'on doit accepter avant de pouvoir les utiliser.
>
> Les licences des programmes privateurs sont très restrictives. Elles empêchent en particulier toute copie et toute modification.
>
> A l'inverse, les licences libres assurent à l'utilisateur l'exercice de ses libertés. Elles assurent aussi que même après modification le programme ou l'œuvre resterons libres.
>
> Exemples de licences libres : GNU GPL, GNU LGPL, GNU FDL, Creative commons cc:by-sa.

Système d'exploitation (operating system = OS)

Ensemble de programmes permettant de faire fonctionner le matériel. En général les systèmes d'exploitation incluent une interface graphique et des outils de base pour l'utilisateur (l'environnement de bureau).

Exemples de familles de systèmes d'exploitation libres : *BSD*, *GNU/Linux.*

Exemples de familles de systèmes d'exploitation propriétaires : *Windows*, *Mac OS.*

Logiciel informatique (software)

Programme destiné à effectuer certaines instructions à la demande de l'utilisateur. Les logiciels font appel au système d'exploitation pour pouvoir faire exécuter leurs opérations par la machine. La plupart des logiciels disposent d'une interface utilisateur graphique (*graphic user interface = GUI*). Certains logiciels ne fonctionnent qu'avec un système d'exploitation donné, tandis que d'autres existent dans différentes versions adaptées à divers systèmes d'exploitations (ils sont dits « multiplateformes »).

Exemples de logiciels libres : *LibreOffice* (suite bureautique), *Mozilla Firefox* (navigateur Internet), *Mozilla Thunderbird* (client de courriel).

Exemples de logiciels propriétaires : *Microsoft Office* (suite bureautique), *Microsoft Internet Explorer, Google Chrome, Apple Safari* (navigateurs Internet), *Microsoft Outlook* (client de courriel).

Paramètres, préférences, personnalisations et options

Les systèmes d'exploitation et la plupart des logiciels permettent aux utilisateurs de choisir un certains nombre d'options (régler des paramètres) afin d'être adaptés aux souhaits de chaque l'utilisateur.

Virus et autres programmes malveillants

Certains programmes sont destinés à effectuer des tâches de destruction de données ou de matériel, d'espionnage (*spyware*) - vol de documents ou de mots de passe - ou permettent de prendre le contrôle d'un ordinateur à distance à l'insu de son propriétaire. Ces programmes sont souvent inclus dans des logiciels qui sont offerts en téléchargement gratuit, ou bien ils se lancent quand on arrive sur une page web piégée. D'autres sont transmis dans des documents joints aux courriers électroniques. Les virus peuvent être transmis sur des supports de données (disques, clé USB, *etc*.) ou au travers des réseaux.

Donnée informatique (data)

Information codée sous forme numérique (*digital*), dans un certain format. Les données sont stockées dans des fichiers. Les données peuvent représenter tout aussi bien le code d'un programme, du texte avec sa mise en forme, des sons, des images fixes ou animées, *etc*. On désigne par le néologisme « multimédia » les données représentant son, image ou vidéo.

L'extension d'un fichier (les derniers caractères situés après le dernier point) renseigne en général sur le format de ce fichier. Mais elle peut être trompeuse.

Exemple d'extensions et de formats ouverts : .ODT (texte OpenDocument), .JPEG (image jpeg), .OGG (son Vorbis), .OGV (vidéo Theora).

Exemple d'extensions et de formats fermés : .DOC (texte *Microsoft*), .TIFF (image tiff), .MP3 (son mpeg-3), .FLV (vidéo *Adobe Flash*).

Réseau informatique (network)

Infrastructure permettant à plusieurs machines de communiquer (échanger des données entre elles). Cette infrastructure peut être composée de câbles ou d'émetteurs et de récepteurs d'ondes électromagnétiques. On distingue les réseaux locaux (*local area*

network = LAN), cantonnés à un espace privé, des réseaux externes qui utilisent des infrastructures de communications publiques.

Client et serveur

On appelle client une machine (ou un logiciel) qui se connecte *via* un réseau à une autre machine (le serveur) qui lui fourni des données. En général le serveur est une très grosse machine qui fourni des données à un grand nombre de clients.

1.2 Dysfonctionnements

Plusieurs types de dysfonctionnements (« *plantages* ») peuvent affecter les différents éléments matériels ou logiciels. Il importe de savoir les reconnaître et les nommer, afin de pouvoir les résoudre ou rechercher efficacement de l'aide.
Dans le cas où un message d'erreur est affiché, en noter le contenu, ainsi que les circonstances de son apparition.
Notez ce que vous étiez en train de faire au moment où le plantage a eu lieu (logiciels et fichiers ouverts, actions en cours, *etc*.). Avant de réessayer une action sur un logiciel, fermer les autres logiciels. En effet si plusieurs logiciels fonctionnent en même temps cela peut finir par saturer la mémoire de l'ordinateur.
Si un logiciel plante régulièrement, prenez l'habitude de sauvegarder votre travail de façon très régulière (certains logiciels peuvent être paramétrés pour faire cela automatiquement).

Perte d'alimentation électrique : échec du démarrage ou extinction brutale

Le moniteur et/ou la machine ne s'allume pas ou s'éteint brutalement.
Il peut s'agir d'une coupure de courant. Celle-ci peut affecter le logement dans son ensemble (coupure du réseau électrique) ou simplement quelques prises, dont celle sur laquelle est branché l'ordinateur (un disjoncteur a sauté, cela peut être du à votre machine ou à un autre appareil électrique branché sur le même circuit électrique).
Si ce n'est pas le cas et que la machine ne peut être remise en route, vérifiez les branchements des divers câbles.
Si la prise est alimentée et que les branchements sont corrects, il peut s'agir d'une panne matérielle.

Blocage (gel / freeze) ou fermeture inopinée du logiciel

Blocage : le logiciel sur lequel vous travaillez ne répond plus aux commandes. Par contre d'autres logiciels continuent de fonctionner.
Cela peut être normal, si vous avez lancé une tâche qui requiert un traitement de longue durée. Si ce n'est pas le cas, et après avoir attendu une minute, essayez de fermer le logiciel.
Fermeture inopinée : la fenêtre du logiciel disparaît brutalement. S'il n'y a pas eu de message d'erreur, vérifiez qu'elle n'est pas simplement minimisée.

Le logiciel ne réalise pas une tâche comme prévu

Assurez vous d'avoir bien compris le fonctionnement de cette tâche et d'avoir bien respecté la procédure à suivre (consultez la documentation si besoin). Si c'est bien le cas, le dysfonctionnement peut être du à une erreur de programmation du logiciel (*bogue* / *bug*).
Aucun logiciel complexe n'est totalement exempt de bugs. Les bugs les plus courants sont connus et documentés. Des solutions de contournement peuvent avoir été publiées. Certains

des bugs signalés sont corrigés soit dans les versions ultérieures du logiciels, soit dans des correctifs (*patch*) qui sont téléchargeables gratuitement.

Blocage ou fermeture inopinée du système d'exploitation

Blocage : aucune action n'est possible, l'ordinateur ne répond plus aux commandes.

Cela peut être normal, si vous avez lancé une tâche système qui requiert un traitement de longue durée. Si ce n'est pas le cas, et après avoir attendu une minute, essayez de fermer ou de redémarrer (*reboot*) le système.

Le plantage du système peut être la conséquence du dysfonctionnement d'un logiciel en cours d'utilisation.

Perte de connexion Internet ou réseau local

Une application Internet ne fonctionne plus (voir chapitre 2 pour les définitions).

Vérifiez que le modem est bien connecté au réseau Internet. Si c'est bien le cas, le dysfonctionnement peut être lié à une perte de la connexion réseau de l'ordinateur. Si toutes les connexions sont fonctionnelles, le problème peut être du soit au dysfonctionnement d'un programme de l'ordinateur, soit – le plus souvent – à une défaillance du service Internet concerné (coté serveur).

2 Introduction à l'Internet

2.1 Principes et définitions

Internet (the Internet)

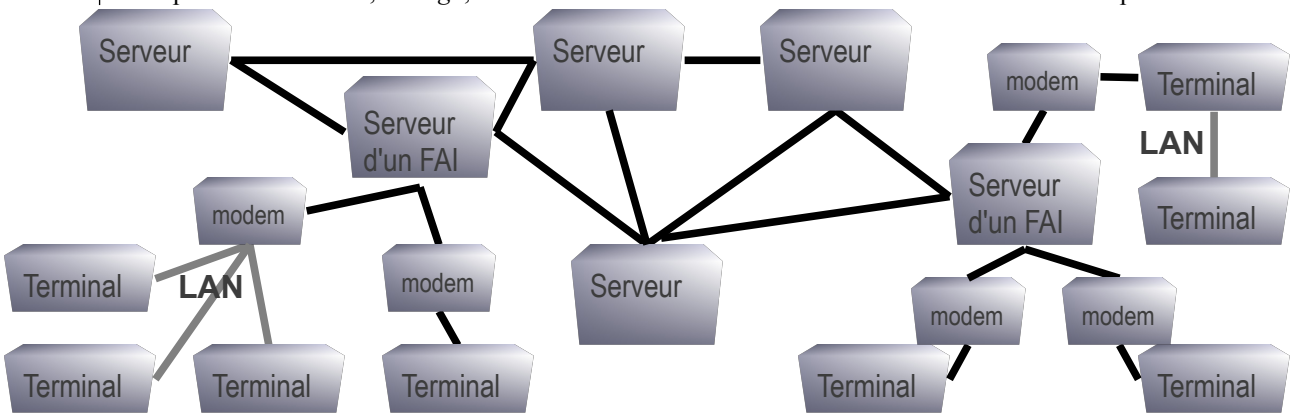
C'est le réseau des réseaux. C'est à dire l'interconnexion de multiples réseaux d'ordinateurs situés sur l'ensemble de la planète. L'Internet est une infrastructure décentralisée composée d'ordinateurs et de leurs moyens de connexion (câbles, émetteurs-récepteurs) ainsi que des programmes et protocoles d'échange de données permettant à ces ordinateurs de communiquer (faire circuler des données entre eux).

Fournisseur d'accès à Internet = FAI (Internet service provider)

Pour accéder à l'Internet, il faut brancher son équipement terminal (PC, tablette, mobile, *etc*.) à un câble (ou à un émetteur-récepteur) qui est raccordé aux serveurs d'une société dite « fournisseur d'accès à Internet ». Ce branchement se fait par l'intermédiaire d'une machine appelée modulateur-démodulateur (modem), parmi lesquelles les « *box* Internet ».

Le FAI permet aux particuliers d'avoir accès au réseau Internet moyennant un abonnement.

Exemples de FAI : *Free*, *Orange*, *SFR*. Chez *Free* l'abonnement haut-débit illimité coûte 30 € par mois.



Dessin 1: Représentation schématique de l'Internet.

Débit de la connexion à l'Internet

Selon les caractéristiques techniques du raccordement au FAI, le débit (quantité de données transmises par seconde) peut être plus ou moins élevé. Cela permet ou non l'usage de certaines applications. Les applications les plus gourmandes en débit sont la télévision, les flux vidéo, le téléchargement de programmes.

Applications et services disponibles sur l'Internet

L'Internet est un réseau au travers duquel peuvent circuler toutes sortes de données. Ces données circulent à l'aide de divers protocoles (langages de communication). A chaque protocole correspond un type d'application (ou service) particulier.

Exemples d'applications : le Web, le courrier électronique, la messagerie instantanée, la voix sur I.P. (téléphonie), l'échange de fichiers décentralisé (peer-to-peer), l'échange de fichiers avec un serveur (FTP), *etc*.

Identification sur l'Internet : I.P., URL et nom de domaine

Chaque équipement connecté au réseau Internet est identifié par une adresse I.P. (*Internet Protocol*). Il n'est donc pas possible d'effectuer des opérations de façon anonyme. (Toutefois un pirate peut utiliser votre ordinateur à votre insu.)

Exemple d'adresse I.P. : 212.85.150.134

Remarque : il existe une solution technique qui permet d'augmenter l'anonymat de la navigation web : le réseau TOR. Mais elle est délicate à utiliser, pas absolument sure et elle ralenti le débit. Peu de personnes l'utilisent.

Chaque ressource (fichier) est identifiée par une adresse URL (*Uniform Resource Locator*).
Exemple : l'URL de la page « Internet » en français de l'encyclopédie libre *Wikipedia* est https://secure.wikimedia.org/wikipedia/fr/wiki/Internet
La première partie de l'URL (à gauche des signes ://) est un schéma qui désigne en général le protocole utilisé (dans notre exemple : HTTPS – qui désigne le protocole hypertexte (application Web) sécurisé). La seconde partie indique l'adresse d'un fichier. Dans cette seconde partie il est utile d'identifier le nom de domaine : c'est la partie qui précède le premier signe / et qui se compose d'une séquence de caractères (délimitée par des points ou des /) suivie d'un point et d'une (ou deux) autre séquence de caractères constituant le « domaine de premier niveau » (*Top-Level Domain = TLD*).
L'URL se présente donc ainsi : schéma://sous-domaine.domaine-de-second-niveau.tld
Le nom de domaine est domaine-de-second-niveau.tld
Dans notre exemple, le nom de domaine est : « wikimedia.org », le TLD est « org ».
En effet le nom de domaine permet d'identifier l'hébergeur du site, c'est à dire de savoir chez qui on se trouve. Le domaine de premier niveau donne une indication sur le type de site ou son pays d'origine (exemples de TLD : org = organisation ; com et biz = commercial ; info = information ; xxx = pornographie ; net = en rapport avec le réseau (ou divers) ; fr = français ; gouv.fr = gouvernement français ; asso.fr = association française ; be = belge ; ch = suisse ; ca = canadien ; eu = européen. Certains TLD nationaux sont utilisés pour leur sonorité : ce sont des domaines de complaisance).

Traces et enregistrement de l'activité sur Internet

Toute activité effectuée sur Internet est enregistrée à de multiples endroits (sur l'équipement terminal, sur les serveurs du FAI, sur les serveurs des sites visités ou des fournisseurs des services utilisés). Il est absolument impossible d'effacer complètement ces traces. Tout ce qui est fait sur Internet est définitif.

Piratage informatique

Le piratage consiste a effectuer des opérations illégales en contournant les dispositifs de sécurité. Un pirate peut en particulier se connecter à un ordinateur qui ne lui appartient pas *via* le réseau Internet. Cela lui permet d'utiliser cet ordinateur à l'insu de son propriétaire (on parle de « machine zombie ») pour commettre d'autres actions illégales tout en dissimulant son identité ; cela lui permet également de voler des informations sur cet ordinateur ou d'en modifier le contenu (par exemple modifier le contenu d'un site web).
Les pirates malveillants (*crackers*), ne doivent pas être confondus avec les *hackers*, animés par des motivations altruistes ou créatrices et qui se conforment à une éthique.

2.2 Risques liés à l'usage de l'Internet

Des organisations ou des individus malveillants agissent sur l'Internet, comme ailleurs.
Ils cherchent en général à réaliser l'un de ces trois types d'opération :

- obtenir de l'argent ;
- obtenir des données personnelles ou confidentielles ;
- propager de fausses informations (rumeurs) ou censurer l'information.

Les risques seront détaillés ci-après en fonction des différentes applications de l'Internet.

3 Niveau A : naviguer sur la Toile

3.1 Principes et définitions

La Toile ou le Web (the World Wide Web)

La Toile est l'ensemble des documents hypertextes reliés entre eux par des liens hypertextes, et hébergés sur les serveurs de l'Internet. Il utilise le protocole HTTP (HTTPS pour les connexions sécurisées). Ces documents sont mis à dispositions sur des sites web. Il existe différentes catégories de sites : sites web classiques, blogs, forums, wiki, réseaux sociaux, sites de partage de fichiers, *etc*.

Tous les sites sont hébergés sur des serveurs de l'Internet. Chaque jour de nouveaux sites apparaissent tandis que d'autres disparaissent.

La Toile est accessible à l'aide d'un logiciel navigateur (appelé aussi en français fureteur ou butineur ; en anglais : *browser*) (exemple : *Mozilla Firefox*).

Site web classique (website)

Les sites web offrent différentes sortes de services. Le plus simple est la mise à disposition de données diverses (documents, fichiers multimédia, fichiers de programmes, *etc*.). Les fichiers peuvent en général être téléchargés (sauvegardés sur l'ordinateur de l'internaute).

Exemples de données : actualité, opinion, avis de consommateur, article scientifique, annuaire, cartographie, prévision météorologique, programme à télécharger, lecture de fichier multimédia.

D'autres services qui supposent une interaction plus élaborée entre client et serveur sont dits « services en ligne ». Certains services ne sont accessibles que si l'on s'y inscrit*.

Exemples : commerce en ligne, traduction en ligne, pétitions en ligne, jeux en ligne, écoute en ligne d'un flux continu (*streaming*) de musique, radio ou télévision, accès distant au service de courriel, listes de diffusion.

Blog

Un blog (ou journal en ligne) est un site composé d'articles. Ceux-ci sont en général ordonnés chronologiquement. Les blogs sont souvent tenus par des individus qui partagent ainsi leurs impressions, opinions et expériences quotidiennes. Il est parfois possible de commenter les articles**.

Forum

Un forum de discussion est un site organisé en sujets de discussions (*topics*) où les internautes peuvent participer à une discussion en déposant (poster) des messages**. Certains forums sont privés, d'autres sont publics. Il est parfois nécessaire de s'inscrire* pour pouvoir poster des messages, voire pour pouvoir lire le contenu du forum.

Wiki

Un wiki est un site qui permet aux internautes de contribuer** à la rédaction collective de documents.

Réseau social (social network)

Un réseau social est un site qui permet d'entretenir des contacts avec d'autres personnes. Il faut nécessairement s'y inscrire*.

Partage de fichiers

Un site de stockage ou de partage de fichiers est un site qui permet aux internautes de déposer (mettre en ligne) des fichiers (*upload*) ainsi que de les télécharger (*download*).

Abonnement (syndication) : flux RSS et podcast

Sur certains sites (notamment les blogs et les forums) il est possible de s'abonner pour recevoir les articles au fur et à mesure de leur parution. Cette possibilité est signalée par l'apparition de l'icône RSS dans la barre de navigation du fureteur.

Le flux (RSS ou Atom) est pris en charge par un logiciel « agrégateur de flux » (cette fonction est par exemple assurée par le client de courriel *Thunderbird*).

Lorsque l'on s'abonne à la diffusion de fichiers multimédia, on parle alors de *podcast* (ou balado-diffusion).

Contrôle parental

Logiciel qui bloque partiellement l'accès à la Toile. Son but est de protéger la personne qui navigue sur la Toile de sites susceptibles de lui nuire (notamment : sites pornographiques qui dégoûtent du sexe ; sites malveillants qui diffusent des virus ; sites commerciaux qui s'approprient les données personnelles ; services dont l'usage peut provoquer l'addiction – notamment : réseaux sociaux et jeux en ligne).

Les contrôles parentaux peuvent fonctionner de deux manières :

- soit avec une liste blanche : seuls les domaines autorisés sont accessibles ;
- soit avec une liste noire : tout est accessibles sauf les sites qui correspondent aux critères définis par la liste noire.

Ces listes peuvent être définies localement par l'administrateur de l'équipement terminal ou par le fournisseur de ce service, à partir de choix prédéfinis.

Aucun contrôle parental n'offre une protection complète, il faut rester vigilant. Le contrôle parental peut parfois bloquer des sites qui ne devraient pas l'être (faux positifs) cela est inévitable.

Notes :
* pour tout ce qui concerne les inscriptions, voir plus loin le chapitre niveau C.
** en ce qui concerne le fait de poster des messages publics, voir plus loin le chapitre niveau D.

3.2 Naviguer sur la Toile

On accède aux ressources de la Toile, soit en suivant un lien hypertexte à partir d'une page web, soit en effectuant une recherche à l'aide d'un moteur de recherche ou d'un annuaire de sites web. En survolant un lien avec la souris, on peut voir s'afficher dans la barre d'état du navigateur l'URL et donc en particulier le nom de domaine du site vers lequel le lien pointe.

Remarque : lorsqu'on accède à un site web, les données que l'on envoie ou que l'on récupère (lecture) transitent par le réseau et peuvent être interceptées (lues et/ou modifiées), ce qui peut poser des problèmes de confidentialité et de fiabilité. Certains sites permettent des connexions sécurisées par le protocole HTTPS (le protocole de sécurisation s'appelle TLS – anciennement SSL) : les informations sont chiffrées. Ce mode de connexion est préférable mais encore peu répandu en dehors des dispositifs de paiement en ligne.

3.3 Utiliser un moteur de recherche

3.3.1 Choisir un moteur de recherche assurant la confidentialité

La plupart des moteurs de recherche (*search engine*) enregistrent toutes les recherches que l'on y effectue. Ceci permet alors de connaître tous nos centres d'intérêts, nos opinions politiques, notre religion, nos maladies, nos pratiques sexuelles, *etc*. Ceci pose un grave problème de confidentialité et de protection de la vie privée.
Il n'existe que trois moteurs de recherche qui assurent en principe la confidentialité des recherches :
DuckDuckGo.com : c'est le plus fiable car il est développé par des organisations de protection de la vie privée.
Startpage.com : il donne accès aux résultats de la recherche du moteur *Google*, sans donner votre identité à la société *Google Inc.* Il est développé par IxQuick.
IxQuick.com : c'est un méta-moteur, c'est à dire qu'il combine les résultats d'un grand nombre de moteurs de recherche (hors *Google*), sans leur communiquer votre identité.

3.3.2 Choisir des résultats pertinents

Le résultat d'une recherche consiste en une liste d'URL.
Un élément important à regarder avant de choisir et de se diriger vers une URL est le nom de domaine, ainsi on sait plus ou moins où l'on va et ce que l'on risque d'y trouver.

3.4 Risques liés à la navigation sur la Toile

3.4.1 Publicité (*advertisement ou ad*)

De nombreux sites se financent grâce à la publicité. Les publicités peuvent être plus ciblées si le site parvient à obtenir des informations personnelles sur l'internaute et notamment s'il parvient à tracer son activité (les autres sites visités) sur la Toile. Cet espionnage se réalise notamment grâce aux *cookies* (fichiers) que certains sites (et les régies publicitaires qui sont présentes sur ses sites) écrivent sur le disque dur de l'ordinateur de l'internaute. Certaines fonctionnalités ne sont accessibles que si un *cookie* est enregistré.
Il est indispensable d'utiliser un bloqueur de publicité et de bloquer au maximum les *cookies*. (Ces fonctionnalités peuvent être incluses dans le navigateur *Firefox* grâce à des extensions).

3.4.2 Usurpation d'identité (*phishing*)

Il existe des sites qui essayent de se faire passer pour d'autres afin de piéger les internautes.

Couramment, lorsqu'un domaine n'est plus utilisé (le site n'existe plus), on est redirigé vers une page qui prétend être le site recherché et présente une liste de liens publicitaires ou dangereux. C'est pourquoi il est important de **toujours bien regarder le nom de domaine dans l'URL**.

3.4.3 Arnaques et pièges

Certains sites présentent des offres qui sont des arnaques.

Exemples : une offre apparemment gratuite mais en réalité gratuite seulement pendant une certaine période ensuite il faudra payer car on s'est engagé pour une longue durée ; un bien ou un service acheté qui ne sera jamais obtenu ou qui ne correspond pas à sa description ou est une contrefaçon.

D'autres invitent à télécharger des logiciels gratuits qui s'avéreront porteurs de publicités ou de virus informatiques.
Ne pas souscrire à une offre et ne pas télécharger de programme informatique que vous n'ayez pas recherché par vous-même. Passez toujours par le site officiel.

Remarque : sous GNU/Linux, si l'on souhaite installer un nouveau programme, on accède directement aux dépôts de logiciels en passant par la logithèque. On ne télécharge quasiment jamais de programme directement sur un site web.

3.4.4 Fausses informations et censure

Certains sites diffusent de fausses informations. Il est important d'identifier la source d'une information (en premier lieu le nom de domaine du site) et de vérifier toute information à partir d'autres sources.
D'une manière générale **toute information se trouvant sur la Toile (ou ailleurs) est sujette à caution et doit être vérifiée.**

Certaines informations peuvent également être obsolètes : en vérifier la date de publication.

D'autres informations sont censurées par certains sites, notamment les sites d'actualités contrôlés par le grand capital. Les avis négatifs de consommateurs d'un site commercial sont aussi souvent passés à la trappe. Il est là encore nécessaire de **diversifier ses sources d'informations**.

La plupart des gouvernements (y compris ceux prétendument « démocratiques ») censurent également la Toile en empêchant l'accès à certain sites depuis leur territoire.

4 Niveau B : communiquer en privé *via* l'Internet

4.1 Principes et définitions

Communications privées

> Les communications privées incluent les échanges téléphoniques, par courrier électroniques, par messagerie instantanée, ainsi que la fonction de « messagerie privée » incluse dans certains forums, sites de réseau social ou autres. Elles incluent aussi les messages envoyés aux administrateurs d'un site web par l'intermédiaire d'un formulaire de contact présent sur le site.

Caractère privé

> Ces messages ne sont pas destinés à être publiés. Ils ne doivent être lus que par l'expéditeur et le ou les destinataires. Les destinataires sont des personnes clairement identifiées.
> Il n'est pas correct de faire état du contenu de conversations privées à des tiers sans l'accord explicite de toutes les personnes concernées.

4.2 Absence de confidentialité

Les communications qui transitent par l'Internet ne sont pas en général chiffrées. De plus elles sont enregistrées à de multiples endroits. Elles peuvent donc être interceptées et écoutées ou lues (voire modifiées) par des personnes mal intentionnées disposant des accès ou des compétences nécessaires. **Aucune information confidentielle ne doit être transmises sur l'Internet**.

Remarque : il existe des possibilités de chiffrement et de signature électronique des courriels (OpenPGP) mais très peu de personnes les utilisent.

4.3 Responsabilité

Envoyer un message privé entraîne une responsabilité morale et légale. Légalement la personne qui poste un message privé est responsable de son contenu. Si la personne est mineure, l'adulte qui est titulaire de l'abonnement à l'Internet (identifié par l'adresse I.P.) est aussi responsable.

La morale condamne – et loi interdit et puni – notamment : l'usurpation d'identité et les menaces de mort.

La loi condamne également la transmission de fichiers contenant des œuvres originales protégées par le droit d'auteur (*copyright* ©), telles que programmes informatiques, textes, musiques, dessins, photographies, reproductions d'œuvres d'art, vidéos, *etc*. Ces œuvres sont la propriétés de leurs producteurs, lesquels s'opposent en général à leur utilisation. Si on veut les transmettre (les inclure dans un message, ce qui consiste à en faire une copie), il faut en obtenir l'autorisation écrite de la part du propriétaire (souvent moyennant finance).
Toutefois il existe des programmes et des œuvres placés sous licence libre (on parle aussi de « *copyleft* ») ou tombés dans le domaine public (par expiration des droits d'auteur). Ceux-ci peuvent être librement transmis et modifiés. Certains sites web regroupent ce type de contenus.

Par ailleurs si on transmet une œuvre que l'on a créé, il faut l'indiquer et être en mesure de prouver qu'on en est bien l'auteur afin d'éviter que d'autres personnes ne se l'approprient. On peut placer l'œuvre sous une licence plus ou moins libre afin de donner au destinataire plus de droits que n'en confère le droit d'auteur.

Exemple : ce document est diffusé sous la licence cc:by-nc-sa. Il n'est pas libre car son utilisation commerciale est interdite (nc), mais vous pouvez le copier, le modifier et diffuser vos modifications sous la même licence (sa) en mentionnant l'auteur original (by).

4.4 Bonnes pratiques pour les messages écrits

Qu'ils soient privés ou publics, les messages doivent être lisibles et compréhensibles.
Éviter le style « SMS » particulièrement irritant pour les lecteurs, ainsi que les abréviations qui ne sont pas toujours comprises par tout le monde. Éviter de même d'abuser des mots écrits en majuscules (ce qui revient à crier). Écrire dans un français correct et en utilisant un vocabulaire précis de façon à éviter les ambiguïtés, les incompréhension ou pire : les contre-sens et mauvaises compréhensions.

Les messages écrits n'étant pas accompagnés de signaux de communication non verbaux, tels que le ton de la voix ou les mimiques du visages, sont lus sans nuances. Une blague peut facilement être prise pour une insulte et d'une manière générale tout contenu désagréable voit son effet décuplé. Il est très facile de se fâcher avec un correspondant. Les émoticônes (*smileys*) : signes textuels ou graphiques (icônes) indiquant des états émotionnels servent à palier *en partie* cette absence de signaux de communications. Il faut néanmoins faire bien attention à ce que l'on écrit et à la façon de le formuler afin d'éviter que le destinataire ne se sente agressé ou blessé.

Note : pour pouvoir utiliser les émoticônes graphiques dans un client de messagerie, il faut rédiger les messages au format HTML. Cela est déconseillé et peu usité car certains clients de messagerie affichent mal ce type de messages.

5 Niveau B.1 : utiliser le téléphone

5.1 Principes et définitions

Le service de voix sur I.P. (VoIP)

La téléphonie par Internet ou « voix sur I.P. » (protocole VoIP) permet l'acheminement de la voix via le réseau Internet. Cela nécessite soit un un appareil téléphonique (un appareil fixe sera directement relié au modem (box) Internet) soit un logiciel client de téléphonie (*softphone*).

Numéros de lignes téléphoniques

En France les numéros ordinaires comportent 10 chiffres.
Les numéros qui commencent par 01, 02, 03, 04 et 05 sont des numéros « géographiques » de ligne téléphonique fixe.
Les numéros qui commencent par 09 sont des numéros de ligne téléphonique fixe VoIP.
Les numéros qui commencent par 06 et 07 sont des numéros de ligne téléphonique mobile.
Les numéros qui commencent par 08, ainsi que les numéros courts sont des numéros « spéciaux » qui donnent accès à des services souvent surfacturés.
Les numéros qui commencent par 00 sont des numéros de lignes d'un pays étranger.

Tarification

L'accès au service VoIP et la tarification des appels dépendent de l'abonnement souscrit auprès du FAI. Certains services accessibles par logiciel nécessitent un abonnement spécifique.
La plupart des forfaits d'accès à l'Internet permettent d'appeler gratuitement des téléphones fixes en France (et dans certains pays). Pour éviter des surcoûts, ne pas utiliser le téléphone fixe (VoIP) pour appeler des téléphones portables (numéros commençant par 06 ou 07). Utiliser de préférence un téléphone portable pour les appeler.
Certains forfaits d'accès à l'Internet incluent aussi les appels vers les portables.
Éviter aussi autant que possible les numéros spéciaux (commençant par 08 ou numéros courts).

5.2 Bonnes pratiques

Tenir compte de l'heure (décalage horaire éventuel) et des habitudes du correspondant avant de l'appeler (faire sonner son téléphone).

5.3 Risques spécifiques à l'usage du téléphone

5.3.1 Usurpation d'identité

Un correspondant au téléphone peut chercher à se faire passer pour quelqu'un d'autre. Il n'y a aucun moyen de vérifier, à moins qu'il ne s'agisse d'un proche dont on peut reconnaître la voix. Le numéro de téléphone peut être reconnu mais ce n'est pas une garantie absolue car le piratage de ligne est possible.

De manière générale il faut éviter de donner des informations si on est pas sur de la personne avec qui on parle.

5.3.2 Sondage et démarchage commercial

Des sociétés de marketing font des sondages par téléphones pour obtenir des informations personnelles. Ils prétendent souvent que le sondage est anonyme : il n'y a aucune garantie que cela soit vrai. Au contraire, comme les informations personnalisées valent plus cher, dans la plupart des cas les sondages ne sont pas anonymes !
D'autres sociétés commerciales tentent de vendre leur produits en vous appelant par téléphone et en tentant de les embobiner.

Dans tous les cas **ne jamais donner d'information. Il est plus simple de ne pas entamer de conversation : raccrocher dès qu'on a compris qu'on a affaire à ce type d'appel**.

Attention : l'usurpation d'identité ou la manipulation commerciale sera d'autant plus efficace si la personne qui appelle dispose d'informations personnelles vous concernant, obtenues notamment sur l'Internet.

6 Niveau B.2 : utiliser le courrier électronique

6.1 Principes et définitions

Le service de courrier électronique (courriel ou e-mail)

> Le service de courriel permet l'échange de messages écrits entre correspondants. Les messages sont distribués dans des boîtes aux lettres électroniques. Ce service utilise les protocoles IMAP, POP et SMTP.
> Le service de courriel est accessible à l'aide d'un logiciel client de messagerie (exemple : *Mozilla Thunderbird*) ou à l'aide d'une application web appelée *webmail*.

Compte de courrier électronique

> Pour pouvoir utiliser le service de courriel il faut ouvrir un compte chez un hébergeur de courriel. L'hébergeur alloue une certaine place sur le disque dur de son serveur pour stocker les courriels. Il donne accès à un logiciel (serveur de courriel) qui permet d'expédier et de recevoir des courriels, ainsi que de les récupérer sur votre ordinateur.
> On peut ensuite définir une ou plusieurs adresses de courriel (*alias* ou redirection) pour recevoir des messages.

URL d'une adresse courriel

> L'adresse courriel est composé d'un identifiant personnel puis du signe arobas @ suivi d'un nom de domaine : il peut s'agir de celui de l'hébergeur du compte ou d'un nom de domaine qui appartient à l'expéditeur (organisme ou personne privée).
> Exemple: l'URL de l'adresse courriel de Toto est mailto://toto@ouvaton.org,. Le nom de domaine est ouvaton.org (il s'agit d'un hébergeur), mailto est le schéma qui indique qu'il s'agit d'une adresse de courriel.

Message (courriel ou e-mail)

> Un message est envoyé par un expéditeur à l'intention d'un ou plusieurs destinataires. Le message transite par divers serveurs (qui sont susceptibles d'en conserver une copie) avant de parvenir à destination.
> Le message comprend un en-tête avec les adresses courriel de ces personnes, la date et l'heure d'expédition ainsi que d'autres informations techniques, notamment un identifiant unique. Le message proprement dit est constitué d'un sujet qui résume son contenu et du corps du message. Une ou plusieurs pièces jointes (fichiers) peuvent être attachées au message.

Destinataires du message

> Une ou plusieurs personnes à qui le message est adressé.

Destinataires en copie

> Une ou plusieurs personnes à qui on adresse une copie du message pour information.

Destinataires en copie cachée

> Une ou plusieurs personnes à qui on adresse une copie du message pour information. Dans ce cas les autres destinataires ne voient pas ces destinataires cachés.

Répondre à un message

> On répond à l'expéditeur du message. Dans le cas où le message était expédié à plusieurs destinataires, l'option « répondre à tous » permet d'envoyer la réponse à l'expéditeur et à tous les destinataires (en copie).

Si c'est un message provenant d'une liste de discussion, il est courant que la réponse soit envoyée à la liste (voir ci-dessous).

Faire suivre un message

Cela consiste à réexpédier tout ou partie du message reçu à d'autres personnes, en y ajoutant en général un commentaire. Il est recommandé d'effacer l'adresse courriel de l'expéditeur pour ne pas la transmettre à des tiers qui n'ont pas à la connaître.

Liste de diffusion et de discussion (mailing-list)

Certains messages sont envoyés à une liste plus ou importante de destinataires qui sont abonnés à cette liste. On peut parfois être abonné contre son gré. Il doit être normalement possible de se désabonner.

Une liste de diffusion est à sens unique : un seul expéditeur envoi des messages aux abonnés (cas notamment des messages d'information ou des messages publicitaires).

Une liste de discussion permet à un groupe de personne d'échanger entre eux des messages qui peuvent être expédiés par n'importe quelle personne du groupe et qui seront à chaque fois expédiés à l'ensemble des membres du groupe (de la liste).

6.2 Bonnes pratiques

6.2.1 Protégez les adresses de vos correspondants

Lorsque vous envoyez un courriel à de multiples destinataires, qui ne se connaissent pas nécessairement entre eux, évitez de divulguer à tous les adresses courriels de tout le monde. Pensez que votre message peut lui même être relayé à bien d'autres destinataires.

Au lieu de mettre votre série de destinataires dans le champ destinataire (à: / pour: / to:) ou dans le champ copie (Copie à: / cc:) mettez les dans le champ copie caché (Cci: / Bcc:).

Mieux : si vous communiquez souvent avec le même ensemble de personnes, utilisez une liste de diffusion ou une liste de discussion. Vous pouvez constituer une liste dans votre logiciel client de courriel ou utiliser un service en ligne de listes.

Si l'on souhaite seulement protéger l'adresse de courriel d'une personne (ne pas la communiquer aux autres destinataires) on peut mettre ce destinataire en copie cachée, tout en précisant dans le corps du message qu'une copie lui est envoyée.

6.2.2 N'envoyez pas de pièce jointe dans un format propriétaire

Un format propriétaire est un format spécifique d'un logiciel. Il peut ne pas être lu correctement par une personne qui ne dispose pas du même logiciel ou pas de la même version du logiciel que vous. C'est typiquement le cas des formats *Microsoft Office* (doc docx xls xlsx ppt pptx pps). Envoyez vos documents dans un format libre, qui permet l'interopérabilité (exemples : odf txt csv pdf html). Ceci vaut aussi pour les formats image, audio, vidéo et archives.

6.2.3 N'envoyez pas de pièce jointe excessivement lourde

Une pièce jointe inutilement lourde encombre le réseau et les boîtes aux lettres de vos destinataires. Si l'un d'eux a un compte qui est proche de la saturation, votre message pourrait bloquer son compte et lui faire perdre les courriels qui suivront.

De manière générale n'incluez jamais d'image non compressée (bmp) ou de son non compressé (wav) dans des documents ou des messages.

6.2.4 Sujet du message

Le sujet doit correspondre précisément au contenu du message (évitez les sujets du genre « salut ! »), ainsi il permettra aux destinataires de mieux classer et retrouver le message au milieu des autres.

6.2.5 Corps du message

Voir § 4.4.

6.3 Risques spécifiques à l'usage du courrier électronique

6.3.1 Courrier indésirables (pourriel ou *spam*)

Dès lors que votre adresse de courriel a été divulguée (notamment sur l'Internet) vous êtes exposé à recevoir des courriel indésirables. Ce sont des arnaques, de la publicité ou de fausses informations (canular ou *hoax*) que vous êtes invité à retransmettre à vos contacts.
Exemples d'arnaques : faire croire que l'on a gagné à un tirage au sort ; proposition pour gagner de l'argent rapidement et facilement ; invitation à s'inscrire sur un site frauduleux pour y retirer un cadeau, bénéficier d'un service ou d'un produit en promotion.
Malgré que les logiciels client de courriel tentent de les détecter et de les classer à part cela devient vite une nuisance. C'est pourquoi il faut utiliser une adresse de courriel spécifique (une redirection) pour s'inscrire à des services web, et prévoir de la changer assez souvent.

6.3.2 Usurpation d'identité (*phishing*)

Parmi les courriel indésirables il en est qui cherchent à obtenir des informations confidentielles ou personnelles (coordonnées bancaires, mots de passe, *etc*.) en faisant croire qu'ils émanent, par exemple, de votre banque, de votre fournisseur d'accès à Internet ou de votre hébergeur de courriel. (Souvent le message annonce que le service n'est plus accessible et qu'il faut se connecter (suivre un lien) pour le réactiver : c'est un piège.)
Ceci peut se détecter d'une part en regardant attentivement le nom de domaine de l'expéditeur (mais cela ne suffit pas car le compte de courriel peut avoir été piraté), d'autre part par la nature du contenu.
Attention : on peut recevoir un courriel indésirable émanant d'un correspondant habituel si son compte de courriel à été piraté.

Ne jamais transmettre d'information confidentielle par courriel. Ne jamais répondre à message suspect, ni cliquer sur des liens qu'il contient, ni ouvrir les pièces jointes qu'il contient.

7 Niveau B.3 : utiliser la messagerie instantanée

7.1 Principes et définitions

Messagerie instantanée (instant messaging = IM ou chat)

La messagerie instantanée permet d'échanger des messages écrits en direct avec un interlocuteur connecté. On peut indiquer à ses interlocuteurs potentiels si on est disponible ou non (statut).

D'autres fonctionnalités peuvent s'y ajouter (si le protocole et le logiciel client sont compatibles avec elles) : discussion à plusieurs, salon public de discussion, transferts de fichiers, tableau blanc collaboratif (*whiteboard*), son, visioconférence, chiffrement des connexions et des messages, *etc*.

Protocole

Contrairement à la messagerie ordinaire (courriel), il existe un nombre important de protocoles de communication par messagerie instantanée. Les protocoles sont incompatibles entre eux. Certains sont libres et ouverts, d'autres sont propriétaires et fermés.

Les protocoles libres sont : XMPP, SIP (spécialisé pour la visioconférence et les appels vers des lignes téléphoniques) et IRC (spécialisé pour les discussions collectives).

Exemples de protocoles propriétaire : MSNP (Microsoft), YMSG (Yahoo), AIM (AOL), ICQ (Mail.ru), Skype (Microsoft).

Réseau, serveurs et comptes

Il existe autant de réseaux de messagerie instantanés que de protocoles, et même plus car certains réseaux utilisent le même protocole. Seuls les réseaux utilisant le même protocole sont compatibles entre eux, à conditions qu'ils ne soient pas fermés.

Pour communiquer, il faut s'inscrire à chaque réseau où l'on a des correspondants ! Ou bien convaincre ses correspondants de s'inscrire au réseau que l'on utilise.

Les réseaux commerciaux sont centralisés : tout passe par les serveurs de la société qui fourni le service. A l'inverse certains réseaux basés sur les protocoles libres sont décentralisés : ils s'appuient sur une multitude de serveurs mis en place par des organismes et des individus. Dans ce dernier cas on s'inscrit sur un serveur particulier (il est parfois possible d'utiliser néanmoins les services assurés par d'autres serveurs).

Il est vivement recommandé d'utiliser exclusivement les protocoles libres et en particulier le réseau décentralisé Jabber, utilisant XMPP.

Les serveurs stockent les messages et la liste de vos contacts. Ils peuvent offrir des services supplémentaires, tels que : passerelles vers d'autres protocoles, salons de discussion, annuaire.

URL d'une adresse de messagerie instantanée

L'adresse IM est composé d'un identifiant personnel puis du signe arobas @ suivi de l'identifiant du serveur qui comprend un nom de domaine : il peut s'agir du domaine de l'hébergeur du compte ou d'un nom de domaine qui appartient à l'utilisateur (organisme ou personne privée).

Si on utilise le réseau Jabber, cet URL est appelée JID (Jabber Identifier).

Exemple: le JID de l'adresse IM de Toto est xmpp://toto@im.apinc.org. Le nom de domaine est apinc.org (il s'agit d'un hébergeur), xmpp est le schéma qui correspond au nom du protocole.

Client de messagerie instantanée

Le service de messagerie instantanée est accessible à l'aide d'un logiciel client de messagerie instantané. Certains logiciels sont multi-protocoles tandis que d'autres sont spécifiques d'un seul protocole (toutefois les logiciels spécifiques de Jabber/XMPP peuvent utiliser des passerelles qui leur permettent de prendre en charge d'autres protocoles (avec parfois des fonctionnalités limitées, notamment pour les protocoles fermés).

Contacts

Il faut ajouter dans sa liste de contact, les adresses des personnes avec lesquelles on souhaite pouvoir discuter. Ces personnes peuvent appartenir à différents réseaux sous réserve que l'on soit soi-même inscrit sur chacun de ces réseaux et que le logiciel client les prenne en charge.

Statut

L'utilisateur du logiciel de messagerie instantanée peut indiquer un statut correspondant à sa présence et sa disponibilité, éventuellement de façon différentiée selon tel ou tel contact.
L'invisibilité permet d'avoir accès aux statuts des contacts tout en apparaissant comme déconnecté.

Carte de visite (vCard)

La carte de visite présente des informations sur le titulaire du compte de messagerie instantanée. Ces données sont publiques, elles sont stockées sur le serveur. Renseigner la carte de visite est facultatif.

7.2 Bonnes pratiques

Les mêmes que celles liés à l'usage du courriel.

7.3 Risques spécifiques à l'usage de la messagerie instantanée

L'usurpation d'identité est possible.
De plus l'usage de la messagerie instantanée peut être très coûteux en temps et conduire à des phénomènes d'addiction.

8 Niveau C : s'inscrire à des sites web ou à des services

8.1 Principes et définitions

Souscription à un service

La souscription consiste à conclure une forme de contrat avec un fournisseur de service, afin de pouvoir bénéficier du service, qu'il soit payant ou gratuit.
Cette souscription nécessite l'acceptation des conditions contractuelles et l'inscription.
Il est indispensable de lire attentivement et complètement ces conditions pour s'éviter de mauvaises surprises.

Inscription

L'inscription consiste à ouvrir un compte sur un site web (par exemple un forum) ou auprès d'un fournisseur de service. Une fois l'inscription effectuée (il est parfois nécessaire de la valider en cliquant sur un lien contenu dans un courriel envoyé automatiquement par le service) il devient possible d'accéder à certaines fonctionnalités (exemple : pouvoir poster des messages sur un forum) ou de bénéficier du service souscrit. Il faudra s'identifier (se connecter) à chaque nouvelle visite du site web.
Note : il est nécessaire d'autoriser les *cookies* du site concerné (voir § 3.4.1) - au moins « pour la session » - lorsque l'on s'inscrit et pour pouvoir ensuite se connecter.

Données personnelles

A minima l'ouverture d'un compte nécessite de fournir une adresse de courriel et/ou un pseudonyme - l'un des deux servira de code de connexion (*login*) - et un mot de passe (*password*) qui sera également demandé lors de la connexion.
Toutefois certains fournisseurs de services peuvent demander d'autres informations personnelles (telles que nom, prénom, adresse postale, téléphone, *etc*.). Parmi celles-ci certaines seront obligatoires pour pouvoir s'inscrire et d'autres seulement facultatives.

8.2 Risques pour la protection de la vie privée

Beaucoup de services sont offerts gratuitement. Pourtant ces services ont un coût (notamment en temps de travail).
En les proposant gratuitement les sociétés cherchent à recueillir des données personnelles qu'elles pourront utiliser pour envoyer de la publicité ciblée et qu'elles pourront revendre à des régies publicitaires ou à d'autres organisations malveillantes. C'est pourquoi beaucoup de sites proposent à l'internaute de s'inscrire (ce qui suppose de donner des informations personnelles).

8.2.1 S'inscrire ou ne pas s'inscrire ?

8.2.1.1 Accéder à des ressources

Tant qu'il s'agit de consulter des ressources mises à disposition gratuitement, il est rarement nécessaire de devoir s'inscrire. Toutefois certains sites invitent l'internaute à s'inscrire en essayant de l'allécher par des offres ou en prétendant « améliorer son expérience » du site. Dans ce cas il n'est nul besoin de s'inscrire.

D'autres sites prétendent obliger l'internaute à s'inscrire pour pouvoir accéder aux ressources qu'ils détiennent. D'autres enfin ne donnent accès à leurs ressources que moyennant finances, la souscription est alors obligatoire. Dans ces cas il est souvent préférable de continuer la recherche afin de voir si ces ressources ne seraient pas accessibles ailleurs librement.

8.2.1.2 Poster des messages ou des contributions publiques

Dès lors qu'il s'agit d'ajouter du contenu à un site, l'inscription est le plus souvent obligatoire.

8.2.1.3 Souscrire à un service

La souscription à un service nécessite une inscription, que le service soit gratuit ou non. Il vaut mieux souscrire un service payant auprès d'une organisation fiable et sans but lucratif que de souscrire le même service gratuitement auprès d'une société commerciale : la gratuité a souvent un coût exorbitant !

8.2.2 Quelles informations donner ?

D'une manière générale donner une information à une personne ou à une société c'est leur donner du pouvoir sur soi. **Il vaut mieux donner le minimum d'informations possible**. Si un site sur lequel on désire s'inscrire demande trop d'informations, mieux vaux y renoncer.
Surtout **ne jamais donner accès à la liste de vos contacts (carnet d'adresse)**.

Les sociétés auxquelles une personne livre ses informations se les revendent entre elles et deviennent capables de les agréger afin de construire un profil de la personne.
Les réseaux sociaux et les moteurs de recherche qui enregistrent toutes nos recherches sont les mieux placés pour construire des profils détaillés. (Les deux sociétés qui exploitent le plus les données personnelles de leurs utilisateurs sont *Facebook* et *Google*. Leur valeur boursière astronomique, alors même que l'essentiel de leurs services sont gratuits, reflète bien la valeur des données personnelles qu'elles recueillent).
Ces profils ont une valeur marchande et intéressent toutes sortes d'acteurs : sociétés commerciales, au premier rang desquelles les régies publicitaires et les sociétés de marketing, « gestionnaires de populations » et police politique, *etc*.

8.2.3 Les options à éviter

Souvent vers la fin du processus d'inscription, il est proposer de s'abonner à des listes de diffusion, le plus souvent publicitaires (elles sont souvent présentées comme diffusion « d'information » ou « d'offres promotionnelles »). Par ailleurs il y a souvent une option qui autorise le site à transmettre vos coordonnées à des tiers. Il faut prendre garde à ne pas autoriser ces options (*opt out*).
Malheureusement certains sites indélicats passent outre.
Le processus d'inscription ne doit pas être effectué à la va-vite. Il faut bien lire tout ce à quoi on s'engage en s'inscrivant. Ensuite il est souvent trop tard pour rectifier.
Remarque : légalement toute personne qui souscrit à un service à distance dispose de 7 jours francs pour se rétracter. Ceci doit se faire par courrier postal recommandé avec accusé de réception auprès du service client. Si vous avez transmis des coordonnées bancaires il est vivement recommander de faire aussitôt opposition auprès de votre établissement bancaire, à tout prélèvement de la part de la société concernée.

8.2.4 Se désinscrire

S'il est très facile de s'inscrire, il est souvent très difficile voire impossible de se désinscrire ! Et encore plus impossible de faire effacer définitivement les données personnelles transmises.
Même résilier un service fourni par une société commerciale peut parfois relever du parcours du combattant.

9 Niveau D : communiquer publiquement sur la toile

9.1 Principes et définitions

Communications publiques

Les communications publiques, incluent les commentaires postés sur un article de blog, les avis postés sur des sites commerciaux ou techniques, les messages postés sur des forums, les messages expédiés sur des groupes de discussion ouverts au public, les contributions à un wiki.

Il est souvent obligatoire de s'inscrire sur le site web concerné avant de pouvoir poster un message. Sur certains sites il est même nécessaire de s'inscrire pour pouvoir lire les messages.

Caractère public

Ces messages ou contributions *peuvent* être lus par un grand nombre de personnes (avec ou sans inscription). Le fait que le message s'adresse à une personne en particulier ne change rien à son caractère public.

Par ailleurs le fait de transférer un message privé à une tierce personne (même par un moyen de communication privé) a un caractère public. De même le fait de dévoiler des informations personnelles concernant une personne - ou de la mettre en cause - à un tiers (même par un moyen de communication privé) peut être considéré un acte ayant un caractère public.

Les lois concernant les publications s'appliquent aux communications publiques.

Charte d'utilisation

Certains sites publient une charte qui comprend les règles à respecter lorsque l'on poste un message. A lire avant de commencer à poster des messages ou contributions.

Modérateur

Personne qui est chargée – sur un site qui accepte les messages des internautes – de veiller au bon déroulement des discussions. Le modérateur intervient pour résoudre des conflits de personnes, pour rappeler à l'ordre des personnes qui ne respectent pas les règles d'utilisation, voire les bannir du site (temporairement ou définitivement). Il peut également supprimer tout ou partie d'un message dont il estime qu'il ne respecte pas les règles.

Modération a priori et a posteriori

La modération d'un message peut avoir lieu soit *a priori* : dans ce cas le message n'apparaît qu'après validation par un modérateur, soit *a posteriori* : dans ce cas le message apparaît tout de suite mais peut être supprimé ou édité (modifié) par la suite.

Dispositifs anti-robots

De nombreux sites utilisent des dispositifs techniques afin de se prémunir des messages indésirables postés par des robots (*bots*). Ces dispositifs demandent en général à l'utilisateur d'effectuer une action (souvent il s'agit de recopier un code difficilement lisible = *captcha*). En effet cette action ne peut être effectuée automatiquement par un robot.

9.2 Responsabilité

Tout ce qui concerne les communications privées s'applique aux communications publiques (*cf.* § 4.3.).
En plus, concernant les communications publiques, la morale condamne – et loi interdit et puni – notamment : l'usurpation d'identité, la diffamation (même sous forme d'insinuation) et l'insulte, les propos discriminatoires (exemples : sexisme, homophobie, xénophobie, racisme), l'appel à la violence et les menaces de mort.

9.3 Bonnes pratiques

9.3.1 Protection des adresses de courriel et respect de la vie privée d'autrui

Ne jamais écrire une adresse de courriel ou un numéro de téléphone (les vôtres ou ceux d'une autre personne) dans un message public. Le faire c'est à coup sur s'exposer à un envoi massif de pourriels. En effet des robots « récolteurs d'adresse de courriel » (*email-harvesters*) parcourent en permanence la Toile à la recherche d'adresses pour alimenter les listes de diffusion de pourriel.
Ne pas dévoiler d'information personnelle sur soi et sur d'autres personnes. Ne pas mettre en ligne de photographie où apparaissent des personnes sans leur consentement explicite.

9.3.2 Contenu des messages

Éviter le hors-sujet : rester dans le cadre défini dans le sujet du forum ou l'article du blog. Éviter les redondances et les répétitions : ne pas créer un nouveau sujet de discussion sur un forum sans avoir vérifié qu'il n'existe pas déjà.
S'il s'agit de présenter une opinion divergente, argumenter et éviter les attaques personnelles. Ne pas répondre aux provocations.
Voir également le § 4.4.

9.4 Risques liées à la communication publique sur la toile

9.4.1 Troll

Les discussions sur les forums sont parfois perturbées par des individus qui jouent la provocation et tentent d'entraîner les participants dans une discussion polémique et stérile. Ces individus sont qualifiés de « troll ». La seule attitude susceptible de décourager un troll est de l'ignorer totalement. En effet le troll est de mauvaise foi et son but est de perturber le forum, pour s'amuser ou pour nuire.
Il est également possible de faire appel à un modérateur pour lui confier la résolution du problème.

9.4.2 Diffamation ou déformation de propos

Dès lors que vous participez à une discussion, vous pouvez faire l'objet d'attaques personnelles, voire de diffamation. Ou bien vos propos peuvent être déformés. Il peut alors être nécessaire d'intervenir pour rétablir la vérité, sans céder à la provocation. On peut s'adresser au modérateur du site si nécessaire.

9.4.3 Censure

Certains sites, sous couvert de modération pratiquent la censure. C'est à dire qu'ils suppriment les messages qui leur déplaisent. Notamment des avis défavorables sur des sites commerciaux, ou des opinions ou informations sociales ou politiques jugées par eux « non correctes » ou « déviantes ». Ce dernier phénomène touche également l'encyclopédie libre *Wikipedia*.
En cas de censure manifeste, il est souvent possible de trouver un autre site approprié où dénoncer ce fait et poster le message censuré.

10 Pour aller plus loin

Pour approfondir et trouver des liens vers des solutions techniques, consultez les fiches pratiques du dossier informatique, proposé par le mouvement pour une écologie libidinale :
http://www.ecologielibidinale.org/fr/fiches/miel-dossier-tic-fr.htm