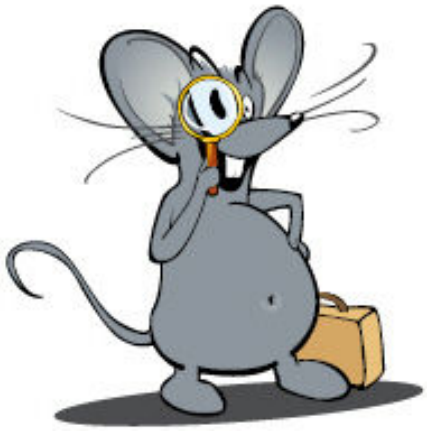
C'est quoi Internet ?



Internet, pour la plupart des gens, est un outil technique que nous utilisons en cas de besoin ; **une source d'information et de communication**. Presque tout le monde voit cette application, qui est liée à un ordinateur et/ou cellulaire (handy, GSM) et un PDA, comme une nouvelle chose technique, tel qu'un baladeur MP3, une console de jeux, une chaîne hi-fi, une télévision, etc.

Mais est-ce vraiment ça ? Eh bien, non ! Certainement pas ! **Internet en combinaison avec un ordinateur (et d'autres appareils ayant la possibilité d'accéder à Internet) représente aujourd'hui toutes les fonctionnalités d'un nouveau mass média**. Mais contrairement à un mass média technique comme la télévision, le mass média le plus connu, qui est **unidirectionnel, Internet est un mass média bidirectionnel.**

Unidirectionnel, bidirectionnel, mais c'est quoi ces expressions ?

Explications pour le terme technique de ces mots.

Unidirectionnel : (Va seulement dans un sens)

Nous poussons sur un bouton et nous recevons quelque chose qui a été programmé sans que nous ayons la possibilité d'intervenir activement.

Exemples pratiques : La télévision, la chaîne hi-fi, le commutateur électrique pour allumer l'éclairage, etc.

Bidirectionnel : (Va dans deux sens, p.ex. question <---> réponse = aussi communication)

Nous poussons sur un bouton et nous recevons **quelque chose qui a été programmé pour que nous puissions intervenir activement** afin de garantir un **dynamisme**. **Quelque chose qui est dynamique est vivante et garantit aussi une continuation (en principe) ! Quelque chose qui est vivante (reproduction, communication, etc.) et dont plusieurs personnes font partie est appelé un « monde ».**

Eh bien, c'est ce qui caractérise Internet ! Internet est un monde, un monde virtuel !

Le nouveau monde, le monde virtuel

Internet est un nouveau monde. Lors de notre naissance, après l'accouchement, nous sommes entrés aussi dans un nouveau monde, le monde réel.
Nous avons dû faire un apprentissage de la vie, apprendre à faire la différence entre le bien et le mal, apprendre les règles fondamentales de la vie et savoir juger les risques.

Le monde virtuel:

Quand nous parlons d'Internet, nous parlons d'un monde virtuel.

Pourquoi virtuel ?

Virtuel parce que c'est un monde qui existe bien, mais qui est *a priori* invisible, un monde créé par des humains, des programmeurs en informatique, un monde que nous pouvons seulement visiter quand nous sommes branchés par une connexion internet, un monde électronique, un nouveau monde à explorer et à essayer de comprendre.

Copyright © by Gust MEES (LU)

Pourquoi pouvons-nous parler d'un monde ?

Quand nous effectuons une connexion à l'internet nous avons recours aux sources suivantes:
Achats, voyages, téléphonie, dictionnaires, échanges d'idées, échange d'informations, discussions, commandes, visites virtuelles de lieux (musées etc.), jeux, photos et bien d'autres encore…

Nous pouvons faire presque tout ce qui est similaire à notre vie quotidienne. Ce monde a été créé par des humains, par nous-mêmes. Il grandit de seconde en seconde. Nous contribuons à le faire grandir et nous grandissons avec lui. Mais l'être humain n'est pas parfait. Bien au contraire. Comme c'est un monde relativement nouveau, il n'existe pas encore de législation internationale.

Avec ce phénomène ressemblant à une action anarchique nous retrouvons sur Internet des choses „**pourries**", comme dans le monde réel, notre monde, notre vie quotidienne. Pourtant l'internet est quelque chose de très bien.

Nous avons droit à la plus grande bibliothèque mondiale et ceci sans heures d'ouverture.

Quand nous visitons l'internet nous entrons à nouveau dans un monde qui nous est inconnu, le monde virtuel.

Ce monde virtuel peut quand même être décrit et comparé avec notre monde réel afin de mieux le comprendre ou de le comprendre vraiment.

Description visuelle de l'internet :

Notre ordinateur est à voir comme le moyen de transport pour naviguer à travers les autoroutes digitales, les « data highways ». Ces autoroutes digitales sont maintenues par les « Fournisseurs d'Accès Internet » (FAI) ou appelés encore « Internet Service Provider » (ISP). Nous payons une cotisation mensuelle pour utiliser ces autoroutes digitales. Ce sont les FAI qui par l'intermédiaire de leurs conditions générales d'utilisation, TOS en anglais (Termes Of Service), en allemand AGB (Allgemeine Geschäfts Bedingungen), qui nous dictent de ce que nous avons droit de faire et aussi de ce qui nous est interdit de faire.

Il me semble que la plupart des internautes n'ont jamais lus ces conditions générales d'utilisation et qu'ils croient que tout est permis et rien n'est défendu. Prenons-en quelques minutes pour lire les conditions générales d'utilisation des P&T au Luxembourg ; les TOS dans d'autres pays et de FAI différents sont plus au moins pareils :

Copyright (C) by Gust MEES (LU)

TOS extraits P&T Luxembourg

Extrait :

LES LIGNES DIRECTRICES POUR L'UTILISATION DE L'INTERNET DES P&T:

VOTRE SÉCURITÉ NOUS IMPORTE !

Pour que vous puissiez travailler en toute tranquillité sur Internet, P&T Luxembourg a élaboré certaines règles pour l'utilisation de l'Internet. Ces règles vous garantissent que votre expérience Internet se passe dans les meilleures conditions possibles. Qui n'a pas déjà entendu parler de « spamming », «spoofing » ou « hacking » ? C'est pourquoi nous avons élaboré nos lignes directrices pour l'utilisation de l'Internet: pour nous donner les moyens de lutter efficacement contre tout abus d'Internet.

LIGNES DIRECTRICES POUR L'UTILISATION DE L'INTERNET

Abuser du système est strictement interdit. En cas d'abus, P&T Luxembourg se réserve le droit de résilier ou de modifier immédiatement l'accès au service Internet et de facturer les frais engendrés par l'abus du système par le client. Ci-après se trouve une liste d'actions définies comme abus du système.

Cette liste n'est pas exhaustive, toute action pour laquelle un doute existe doit être soumise à P&T Luxembourg pour évaluation (tél.: 12422 (gratuit); fax: 12423 (gratuit); e-mail: internet@ept.lu).
Les actions qui constituent un abus du système comprennent, mais ne se limitent pas à:

1. toute tentative de contourner les mesures d'authentification des usagers ou de sécurité de tout hôte (ordinateur qui exécute des applications), réseau ou abonnement de P&T Luxembourg ou d'Internet en général ("cracking");

2. toute tentative, quelle qu'en soit la nature, pour interférer avec ou de refuser le service à tout utilisateur ou hôte sur Internet;

3. la contrefaçon de courrier électronique ou de messages USENET, de quelque manière que ce soit;

4. l'envoi de quantités volumineuses de courriers électroniques non sollicités ("junk mail", "spamming"); ceci comprend l'inclusion ou la tentative d'inclusion d'adresses de courrier électronique à toute liste d'envoi pour courrier électronique sans l'accord préalable et explicite du destinataire;

5. transférer ou envoyer des "chaînes de lettres" (transferts multiples) de quelque nature que ce soit;

6. l'envoi de messages non appropriés aux groupes de nouvelles USENET, p.ex. l'envoi sans discrimination d'un nombre élevé de messages non sollicités ("spamming") à des groupes de nouvelles ou l'envoi de fichiers binaires encodés à des groupes de nouvelles USENET dont le nom n'indique pas clairement qu'ils existent à cette fin;

7. la tentation d'annuler, de remplacer ou d'interférer autrement avec du courrier électronique ou des messages USENET autres que ceux qui sont originaires du client même;

8. le harcèlement, qu'il résulte du langage, de la fréquence ou de la taille du message;

9. l'utilisation d'un accès chez un autre ISP pour promouvoir un site web de P&T Luxembourg d'une manière non appropriée et/ou abusive;

Copyright (C) by Gust MEES (LU)

10. l'utilisation d'un accès ou d'une connexion réseau de P&T Luxembourg pour rassembler des réponses à des messages envoyés via un autre ISP qui ne respectent pas les présentes règles ou celles de l'autre ISP;

Texte complet P&T Luxembourg :

http://www.ept.lu/upload/FRWDES67ED34/CE7CB9AFF47B/downloads/10938F1916C10.pdf

---

Les FAI peuvent être vus comme le contrôle technique, puisqu'ils nous dictent leurs restrictions dans leurs contrats. Mais en revanche de notre payement mensuel, nous ne recevons pas la protection nécessaire pour naviguer en toute sécurité, sauf contre payement, proposé par certains **FAI** (ex. :P&T Luxembourg), http://www.ept.lu/?lm1=CE7CB9AFF47B, nous avons tout juste le droit d'utiliser les autoroutes digitales, mais pas le droit d'être protégé contre d'autres moyens de transport qui ne correspondent pas aux normes de sécurité, c'est-à-dire les ordinateurs contaminés. À voir comme des voitures dangereuses du point de vue technique. Par exemple, des voitures qui perdent de l'huile, qui ont des fuites et représentent donc un danger immédiat.

D'autres voitures peuvent déraper et produire de cette façon des bouchons, ce qui bloque le trafic. Et c'est exactement ce que font les ordinateurs contaminés sur Internet. Ils font ralentir le flux d'informations sur ces autoroutes digitales par l'envoi de spam en masse.

On pourrait voir (visualiser) le « **spam** » (**courrier non sollicité**) de cette façon. De ces ordinateurs infectés, des « **PC zombies** », est envoyé le courrier non sollicité. I**ls ont une fuite (trou de sécurité)** qui met en danger de sécurité aussi les autres ordinateurs. Le courrier non sollicité (**spam**) de nos jours ne contient plus seulement des offres commerciales de toute sorte d'articles (la plupart du temps du contenu sexuel, offres de drogues et de médicaments, stock quotes, musique et vidéos à télécharger, Nigeria connection, etc.) mais est entretemps aussi employé pour installer des troyens (**chevaux de Troie, trojan**) http://www.internetmonitor.lu/download/04_Troyens.pdf, et d'autres sortes de malware qui contaminent l'ordinateur des personnes ayant ouvert ces courriers électroniques. Ces ordinateurs contaminés refilent leurs virus et malware aussi aux autres internautes. En plus de ceci un ordinateur contaminé « **PC zombies** » devient automatiquement intégré dans le réseau de ce « **botnet** » dès connexion à Internet, même sans avoir ouvert la messagerie électronique. Par les ports ouverts de ces « **PC zombies** » toute communication entre et sort ! Il n'y a pas de portier (firewall, pare-feu) qui les empêche de rentrer et de sortir. Quand les updates (mises à jour) du système d'exploitation n'ont pas été faites, le firewall ne sert plus à grand-chose ! Il y aura des vulnérabilités, des trous de sécurité !

Un ordinateur infecté et qui fait partie d'un réseau de PC-zombies, d'un « botnet » essaie de trouver d'autres ordinateurs contaminés. Il envoi des signaux pour détecter ces autres PC-zombies et se fait automatiquement intégrer dans ce réseau créé par la mafia informatique.

Est-ce que votre ordinateur est un « PC zombie » ?

http://www.internetmonitor.lu/Votre-PC-est-il-un-zombie-a-louer-_a277.html

Nous vivons dans un monde commercial, ceci étant un fait, mais payer pour chaque service sécuritaire je ne suis plus d'accord du tout. Ne serait-ce pas usuraire ? La sécurité devrait être garantie à un minimum quand même, même qu'une sécurité à 100% n'existe pas et est illusoire ! Il existe aussi les logiciels du libre, l'Open Source et le freeware qui devraient être mis en vitrine !

Prenons comme exemple :

Firewall : ZoneAlarm® http://www.zonelabs.com

Antivirus : Avast http://www.pcastuces.com/logitheque/avast.htm

Copyright © by Gust MEES (LU)

Il me semble que les FAI (ISP) devraient prendre plus de responsabilités et mettre en quarantaine les ordinateurs contaminés. Ils devraient envoyer une lettre aux propriétaires des ordinateurs contaminés, leurs expliquant que leur ordinateur n'est pas sécurisé et en même temps leur proposer comment procéder, par des liens pointant envers des sites de sécurité avec des produits gratuits (freeware, open source) et des produits payants.

En ce qui concerne le courrier non sollicité (spam), les FAI ont la possibilité de réduire le trafic autorisé à un minimum, ce qui bloquerait déjà l'envoi en masse par un simple compte de messagerie.

Ces ordinateurs « **zombies** » (**PC zombies**) devraient être remis en état de bon fonctionnement sécuritaire dans un délai prévu, faute d'être déconnecté du réseau, la limite de temps écoulée. **Internet a un impact direct avec le monde réel, les dégâts engendrés par ces ordinateurs infectés coûtent de l'argent, beaucoup d'argent. Néanmoins une assistance technique par les FAI est de rigueur pour aider les internautes à remettre leurs ordinateurs en état de sécurité !**

Ceci n'est pas de la fiction, l'Australie a introduit cette procédure l'année dernière, en novembre 2005 http://www.internetmonitor.lu/L-Australie-deconnecte-les-PC-infectes_a572.html.

Cette action eût tel succès qu'il en sortait le code « **Internet Industry Spam Code Of Practice** » pour les **FAI**, registré auprès de l'autorité australienne des communications et des médias, « **A**ustralian **C**ommunications and **M**edia **A**uthority » !

Le communiqué de presse, « **media release** », complet de l'**ACMA** peut être lu à l'adresse URL suivante :

http://www.acma.gov.au/ACMAINTER.1048806:STANDARD::pc=PC_100882

Récapitulatif :

Internet (monde virtuel) a un impact direct sur notre vie réelle. La sécurité de notre vie réelle est réglée par des lois et des services gratuits que nos **gouvernements sont censés** à fournir afin **de garantir la protection des citoyens**. Puisque Internet a un impact direct sur la vie réelle, il me semble pas plus que normal que l'état s'occupe sérieusement aussi de la sécurité de la vie virtuelle, et/ou impose des lignes de conduite aux FAI !

L'Australie est un exemple de bonne pratique, qui mérite d'être appliqué aussi dans les autres pays !

Mais nous devons aussi nous-mêmes prendre nos responsabilités pour nous balader dans le monde virtuel, tel que nous devons assumer nos responsabilités dans le monde réel ! Les internautes (nous) doivent être conscients quand ils cliquent sur « **oui** » dans le formulaire d'inscription pour recevoir un compte internet **qu'ils ont signés un contrât** !

Nos responsabilités dans le monde virtuel :

http://www.internetmonitor.lu/download/05_NosResponabilite.pdf

Il serait à souhaiter que d'autres gouvernements suivent cette initiative afin de garantir un Internet plus intègre !

N'oublions surtout pas nos enfants ! Ils doivent utiliser Internet dans le domaine éducatif pour faire leurs recherches et devoirs. Pensez à vos responsabilités envers eux ! Ceci est un argument sérieux pour dialoguer avec le gouvernement et les autres acteurs de la scène !

La sécurité ne se discute pas, elle s'applique !

Copyright © by Gust MEES (LU)