

Informatique

Réseau et sécurité

Cours 1 v1.3

Objectifs pédagogique

- Notions sur les communautés virtuelles
- Notions sur les réseaux informatiques
- Notions sur le modèle Internet
- Notions sur la sécurité informatique

Contenu du cours

- I. Bonnes pratiques
- II. Communautés virtuelles
- III. Généralités sur les réseaux et le modèle Internet
- IV. Sécurité informatique

Pré-requis

- Utiliser l'outil informatique de manière régulière
- Utiliser Internet de manière régulière
- Conscience d'existence de « hackers »

I. Bonnes pratiques

- I. Bonnes pratiques
- II. Communautés virtuelles
- III. Généralités sur les réseaux et le modèle Internet
- IV. Sécurité informatique

Prise de conscience

- L'espacement des rails au USA : 4 pieds et 8.5 pouces ?



Les 7 lois générales du temps

1. Loi de **Parkinson** : le travail se dilate jusqu'à remplir la durée disponible pour son accomplissement
2. Loi de **Douglas** : dossiers et documents s'entassent jusqu'à remplir l'espace disponible pour leur rangement
3. Loi de **Pareto** : l'essentiel prend 20 % du temps...
l'accessoire 80 %
4. Loi de **Murphy** : rien n'est aussi simple qu'il n'y paraît
5. Loi de **Illich** : au delà d'un seuil de travail horaire, le temps passé n'est plus efficace
6. Loi de **Carison** : faire un travail en continue prend moins de temps qu'en plusieurs fois
7. Loi de l'**Ecclésiaste** : il y a un moment pour tout et un temps pour chaque chose

II. Communautés virtuelles

- I. Bonnes pratiques
- II. Communautés virtuelles
- III. Généralités sur les réseaux et le modèle Internet
- IV. Sécurité informatique

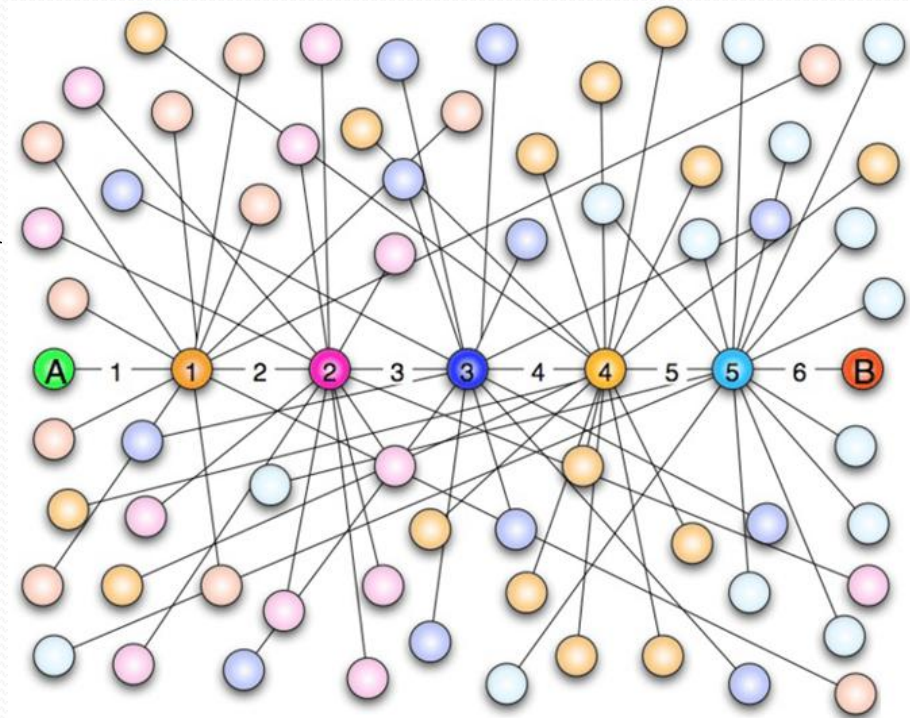
Réseau social

- Ensemble d'**identités sociales** (individus ou groupes) liées entre elles en **réseau** par des **interactions sociales**
- **Médias sociaux** : flux (RSS), blogues, wikis, partage de photos (Flickr), vidéo-partage (YouTube), podcasts, « réseaux sociaux », mondes virtuels, microblogues, etc.
- **Règle des 150** (nombre de Dunbar - 1993) :
 - Nombre d'amis avec lesquels une personne peut entretenir une relation stable à un moment donné de sa vie
 - Au delà, il faut une structure hiérarchique et des règles
- Sur Internet :
 - Amical : Facebook, MySpace, Twitter, Habbo, Trombi, etc.
 - Professionnel : LinkedIn, Viadeo, Xing, etc.

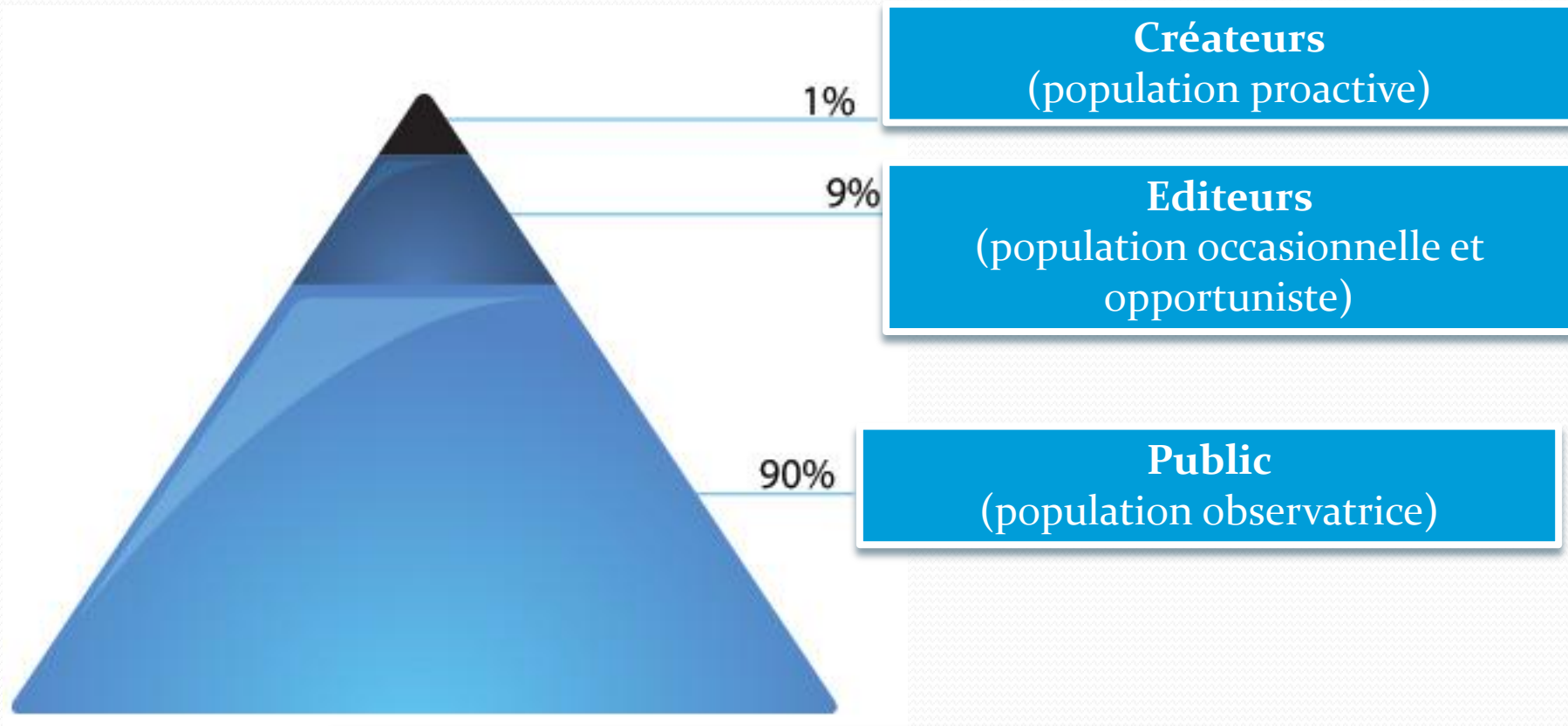
En 2010 : utilisé par 2% des DRH français contre 45% aux États-Unis !

Effet du « petit monde »

- **Paradoxe de Milgram (1967)** : toute personne dans le monde peut être reliée à n'importe quelle autre avec 5 intermédiaires maximum
- Degré de séparation moyen constaté sur Facebook et WLM : 6,5 !



Règle du 1% / Règle 90 – 9 – 1



Règle valable pour toute communauté virtuelle

III. Généralités sur les réseaux et le modèle Internet

- I. Bonnes pratiques
- II. Communautés virtuelles
- III. Généralités sur les réseaux et le modèle Internet
- IV. Sécurité informatique

Adresse IP (Internet Protocol)

- « **Numéro** » d'identification unique attribué à chaque **interface avec Internet** :
 - Ordinateur
 - Téléphone portable
 - Console de jeu
 - Routeur (intermédiaire de routage)
 - Etc.



Formats d'adresse IP

- IPv4
 - 4 nombres de 0 à 255 sous la forme (système décimal)
 - xxx.xxx.xxx.xxx
 - Adresse privée (réseau local : LAN) :
 - 10.0.0.0 à 10.255.255.255
 - 172.16.0.0 à 172.31.25.255
 - 192.168.0.0 à 192.168.25.255
 - Adresse publique (réseau étendu : WAN) :
 - toutes les autres adresses
- IPv6 : le futur ?

Epuisement de IPv4 (IPv6 ?)

December 1990

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

XXX Unallocated
 XXX Allocated/Reserved

IPv4:

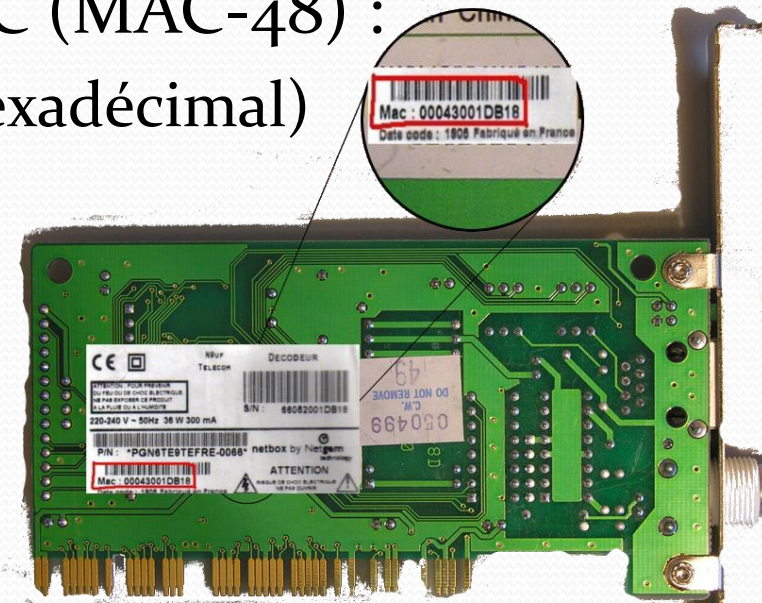
10.1.2.3
 ↓ ↓ ↓ ↓

IPv6: 2002:0A01:0203::/48

IPv6 : Hexadécimal (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B C, D, E, F)
 2001:0db8:0000:85a3:0000:0000:ac1f:8001

Adresse MAC

- Adresse MAC $\neq$ adresse IP
- « Numéro » d'identification unique **physique**
- Exemple de format d'adresse MAC (MAC-48) :
 - 6 nombres de 0 à 255 (système hexadécimal)
 - XX:XX:XX:XX:XX:XX
 - XXXXXXXXXXXXX
 - Exemples :
 - 00:04:30:01:DB:18
 - 00043001DB18



Adresse IP et nom de domaine

- Nom de domaine (**DN**) : identifiant de domaine Internet
- **Domaine** (premier niveau ou TLD) : .com, .org, etc.
- **Sous-domaine** : www, etc.
- **DNS** (Domain Name System) : **service** permettant d'établir une correspondance entre une (ou plusieurs) **adresse(s) IP** et un **nom de domaine**
- Exemple :
 - Adresse IP : 66.249.92.104
 - Nom de domaine : www.google.com

Architecture client/serveur

- Client contact l'adresse **IP** du serveur
- Se connecte à un service (**HTTP**, **HTTPS**, etc.)
- Types de protocoles de communication :
 - **TCP** (Transmission Control Protocol) : mode connecté
 - **UDP** (User Datagram Protocol) : mode déconnecté



© Colopix.be

Analogie avec la distribution du courrier:

TCP : recommandé AR

UDP : courrier simple

Port (logiciel)

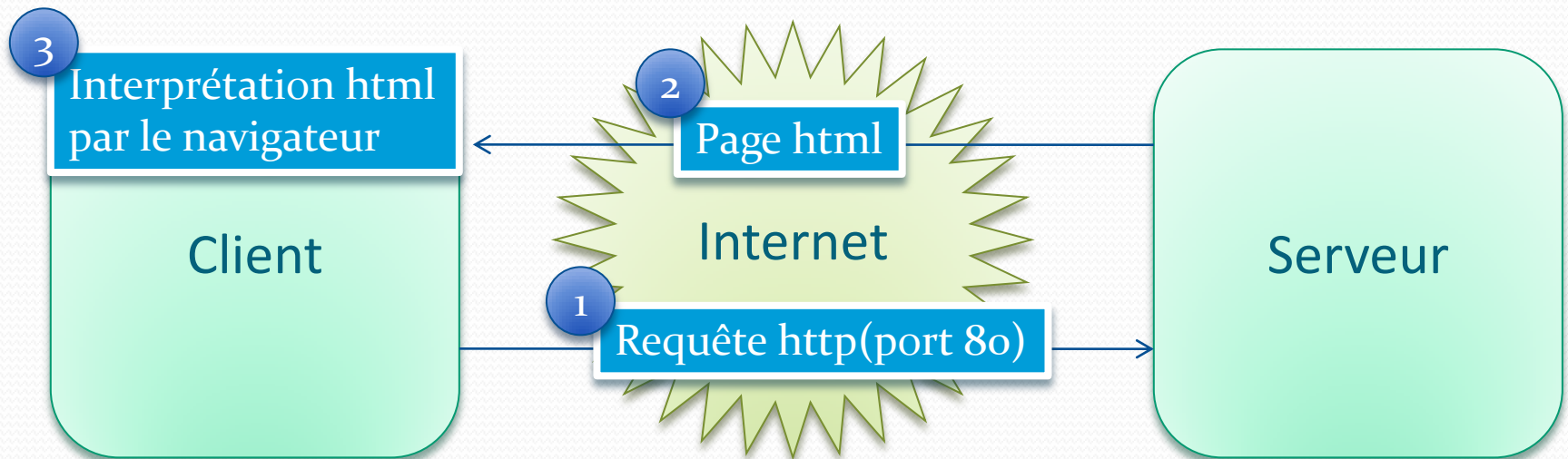
- « Portes » donnant accès au système d'exploitation
- Identifié par un numéro (de 1 à 65535)
- Quelques ports :

Port	Type	Service
53	UDP	DNS
80	TCP	HTTP
8080	TCP	HTTP alternatif

- Exemple :
 - Adresse IP : 66.249.92.104:80
 - Nom de domaine : www.google.com:80

Navigation Web

- HTML (HyperText Markup Language)



Pile de protocoles

Modèle OSI

- 7 – Application
- 6 – Présentation
- 5 – Session
- 4 – Transport
- 3 – Réseau
- 2 – Liaison
- 1 – Physique

Modèle Internet (ou TCP/IP)

HTTP, HTTPS, DNS

TCP, UDP

IP

Ethernet, Wi-Fi, Bluetooth

ADSL

- 5 – Application

- 4 – Transport

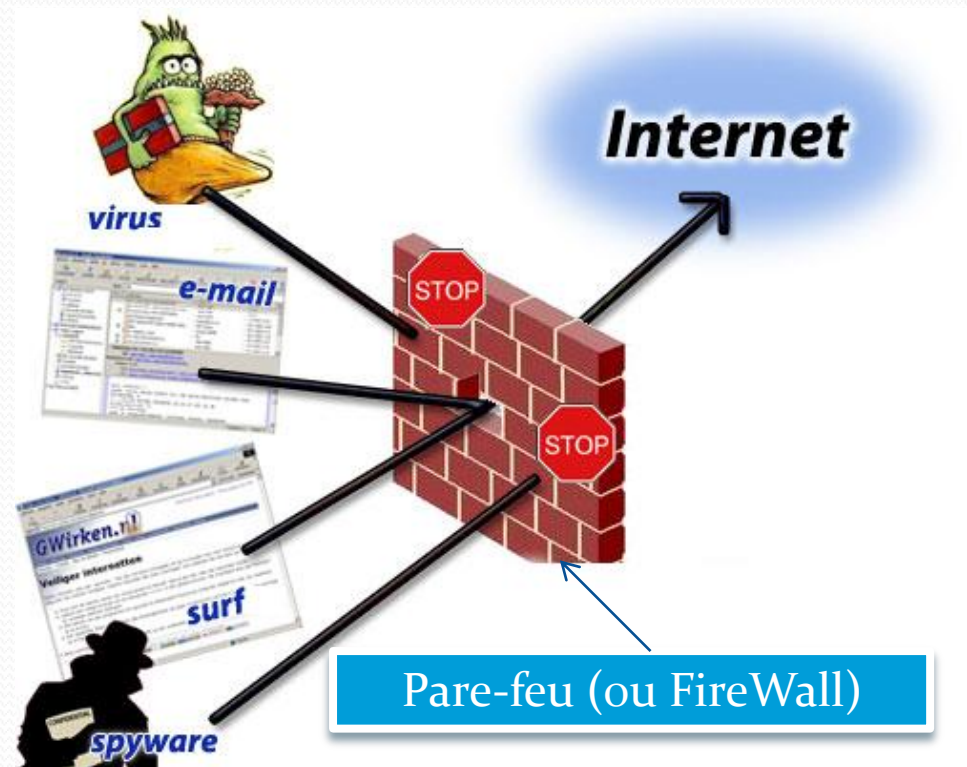
- 3 – Réseau

- 2 – Liaison

- 1 – Physique

Pare-feu (informatique)

- Logiciel / matériel qui a pour fonction de respecter la politique de sécurité du réseau (privé)



IV. Sécurité informatique

- I. Bonnes pratiques
- II. Communautés virtuelles
- III. Généralités sur les réseaux et le modèle Internet
- IV. Sécurité informatique

Généralités

- L'information est partout :
 - De plus en **plus de données**
 - Des données de plus en **plus importantes**
- Connaître le système d'information pour le protéger
- Savoir identifier la menace
- Instaurer de bonnes pratiques de sécurité :
 - Sécurité d'un système = sécurité du maillon le plus faible
- **Auditer** son système
- Apprendre à se défendre : **Ethical Hacking**



Famille de « Hackers »

- « **Script Kiddies** » (pirates néophytes)
- « **Black hats** » (hors la loi)
- « **White hats** » (but « honorable »)
- « **Gray hats** » (mélange de Black et de White hats)
- **Hackers universitaire** (militants Open Source)
- Pirates ? Steakers, Jumpers, etc.



Ingénierie sociale

- Cible du « piratage » : l'**être humain** (tous concernés)
- Attaquant : charismatique, manipulateur, imposteur
- Moyens utilisés :
 - Téléphone, fax, email, courrier, « TailGating », etc.
- Contre-mesures :
 - **Matrice de sensibilité** : régit l'accès aux informations
 - Détecter les attaques : se demander pourquoi ?
 - **Sensibilisation** générale (même standardistes, stagiaires...)

Leviers de l'ingénierie sociale

- Leviers psychologiques :
 - **Absence de méfiance** : pas forcément besoin de dialogue
 - **Crédulité** : utilisation d'un faux prétexte (argent ou gain facile)
 - **Ignorance** : non-sensibilisation à la sécurité des collaborateurs
 - **Confiance** : favoriser le réflexe d'échange (fausse identité, etc.)
 - **Altruisme** : susciter l'envie d'aider
 - **Besoin d'aide** : faire croire que la cible a besoin de notre aide
 - **Intimidation** : créer une situation de peur ou de doute
 - Autres leviers :
 - **Hijacking** : détournement physique d'une personne
- Souvent appelé old-school hijacking (méthode à l'ancienne !)**

Virus, spywares, chevaux de Troie

- **Virus** : logiciel malveillant se reproduisant grâce à un programme hôte :
 - Classique
 - Virus de boot
 - Macrovirus (macro Excel, etc.)
- **Ver** : se reproduit juste grâce au système, se propagent par le réseau, a des actions discrètes et non-destructrices
- **Spyware** : logiciel espion (collecte les données et les envoie à un tiers : hacker ou entreprise)
- **Cheval de Troie** :
 - Création de backdoor, ne se reproduit pas



Bonnes pratiques

- Mot de passe **complexe** (bios, session, etc.) :
 - Long (plus de 6 caractères)
 - Caractères alphanumériques (a-z, 0-9) + caractères spéciaux
 - Pas de mot existant, date de naissance, nom du conjoint...
- Changer souvent de mot de passe
- Interdire les boots autres que disque dur
- **Verrouiller sa session** utilisateur en cas d'absence
- Utilisation d'**antivirus** et d'**anti-spyware**
- **Mise à jour automatique** des logiciels
- Faire des sauvegardes / backups des données

Sécurité informatique : conclusion

- Difficile d'être en sécurité
- les Hackers ont **toujours** une longueur d'avance !
- Ne pas s'attirer les foudres (**éthique correcte**)
- Faire preuve d'**humilité**

Liens

- Livres:
 - Sécurité informatique – Ethical Hacking, ACISSI
- Documents :
 - Éléments de gestion de projet, Gilles Boulet
- Site web :
 - <http://landofthefreeish.com/security/top-500-worst-passwords-2008/>

Crédits

- Auteurs :
 - Mickaël Martin Nevot : **`mmartin.nevot@gmail.com`**