Sécurité des
MÉDIAS SOCIAUX

1 - Web Social : Web 2.0, Médias sociaux et Réseaux sociaux

2 - Le phénomène Facebook

3 - Risques et menaces des Médias sociaux

4 - Les pièges plus répandus

5 - Conseils pour un usage sûr et avisé du Web social

6 - Conclusions

1 – WEB SOCIAL : WEB 2.0

L'évolution d'Internet, le **Web 2.0**, a donné lieu à une nouvelle approche, qui dépasse la simple consultation des sources et où chacun/e peut désormais contribuer avec son propre contenu et le partager, sans compétences techniques particulières, en le rendant instantanément accessible à tous.

« La possibilité d'avoir accès à des services économiques permettant aussi aux utilisateurs peu alphabétisés d'éditer leurs pages est une étape importante vers une interaction et un partage véritables, où le rôle de l'utilisateur devient central. »

(it.wikipedia.org)

1 – WEB SOCIAL : MÉDIAS SOCIAUX

Le **Web 2.0** se caractérise par la possibilité immédiate de créer et partager des contenus grâce à un large éventail d'outils en ligne, les **Médias sociaux**.

« Média social est un terme générique indiquant des technologies et des pratiques adoptées en ligne par les utilisateurs pour partager leurs contenus, textes, sons, images et vidéos. »

(it.wikipedia.org)

Différentes formes de partage : blogs, chats, forums, bookmarking social, wikis, podcasts, sites de partage vidéos et photos, mondes virtuels, **Réseaux sociaux**, …

1 – WEB SOCIAL (en chiffres)

25 MILLIARDS.
Quantité de **contenus** (liens Web, actus, billets, notes, photos, etc.) **partagés chaque mois** sur **Facebook**.

24 HEURES.
Durée totale des **vidéos chargées chaque minute** sur **YouTube**.

2 MILLIARDS.
Nombre de **vidéos vues chaque jour** sur **YouTube**.

27 MILLIONS.
Nombre moyen de **"tweets" par jour** sur **Twitter**.

4 MILLIARDS.
Nombre d'**images** hébergées sur **Flickr**.

*(What the F**K is social media now?)*

1 – WEB SOCIAL : RÉSEAUX SOCIAUX

Les **réseaux sociaux** ont vu le jour dans le but de gérer des réseaux de relations sociales. Ils permettent l'accès à des communautés thématiques, rassemblées autour de leurs passions ou de leurs intérêts "métiers", et de créer de nouveaux contacts amicaux ou d' affaires via les profils personnels ou professionnels.

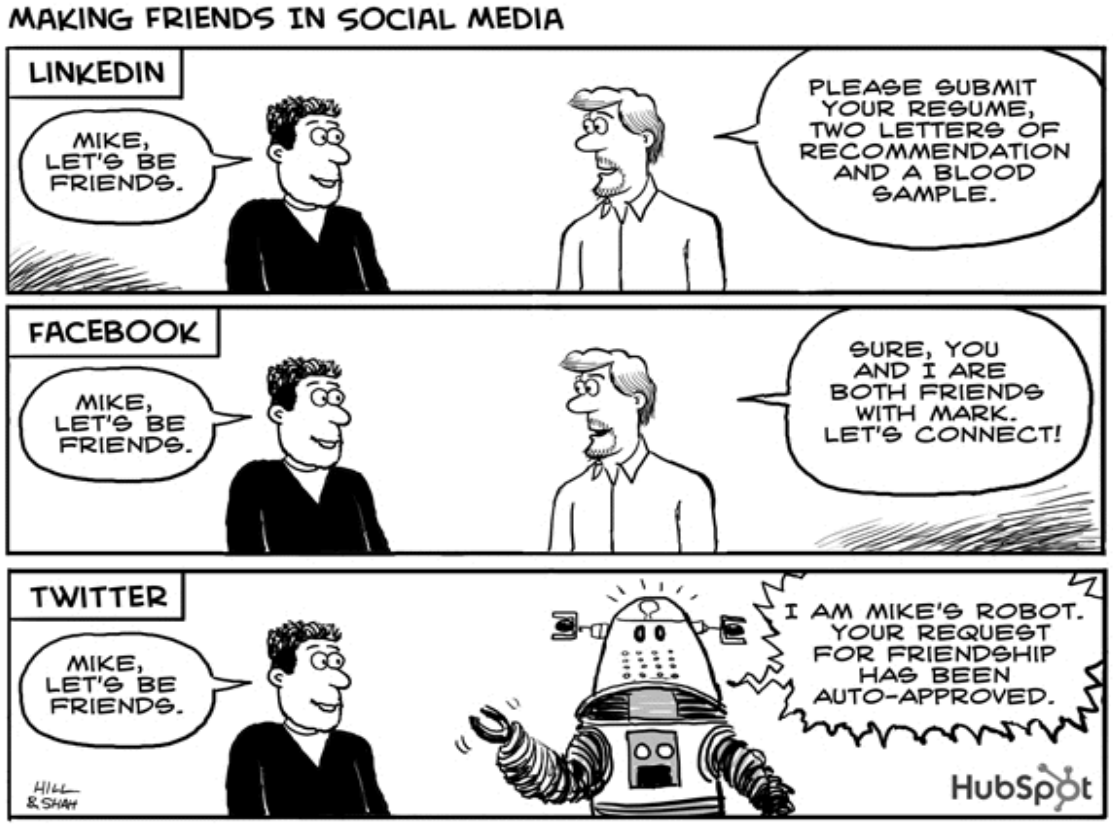
« Réseaux sociaux et networking communautaire créent de nouvelles approches au travail, innovantes, au sein des organisations de la société civile. »

(it.wikipedia.org)

1 – WEB SOCIAL


Social Bookmarks
Comment & Reputation
Crowdsourced Content
Blog Platforms
Blogs/Conversations
Blog Communities
Micromedia
Lifestreams
Specific to Twitter
SMS/Voice
Social Networks
Niche Networks
Customers Service Networks
Location
Video
Video Aggregation
Documents
Events
Music
Wiki
LiveCasting - Video and Audio
Pictures
The Conversation
The Art of Listening, Learning, and Sharing
Brought to you by Brian Solis and JESS3

1 – WEB SOCIAL



« Dès 2014, pour 20% des utilisateurs professionnels, les services des réseaux sociaux remplaceront l'email comme principal vecteur des communications interpersonnelles. »

(Gartner Reveals Five Social Software Predictions for 2010 and Beyond)

2 – LE PHÉNOMÈNE FACEBOOK

Facebook est un phénomène unique, compte tenu du degré de densité de sa diffusion à l'échelle mondiale.

« Si Facebook était un pays, ce serait le troisième pays plus peuplé au monde, devant les États-Unis et juste derrière la Chine et l'Inde. »

*(What the F**K is social media now?)*

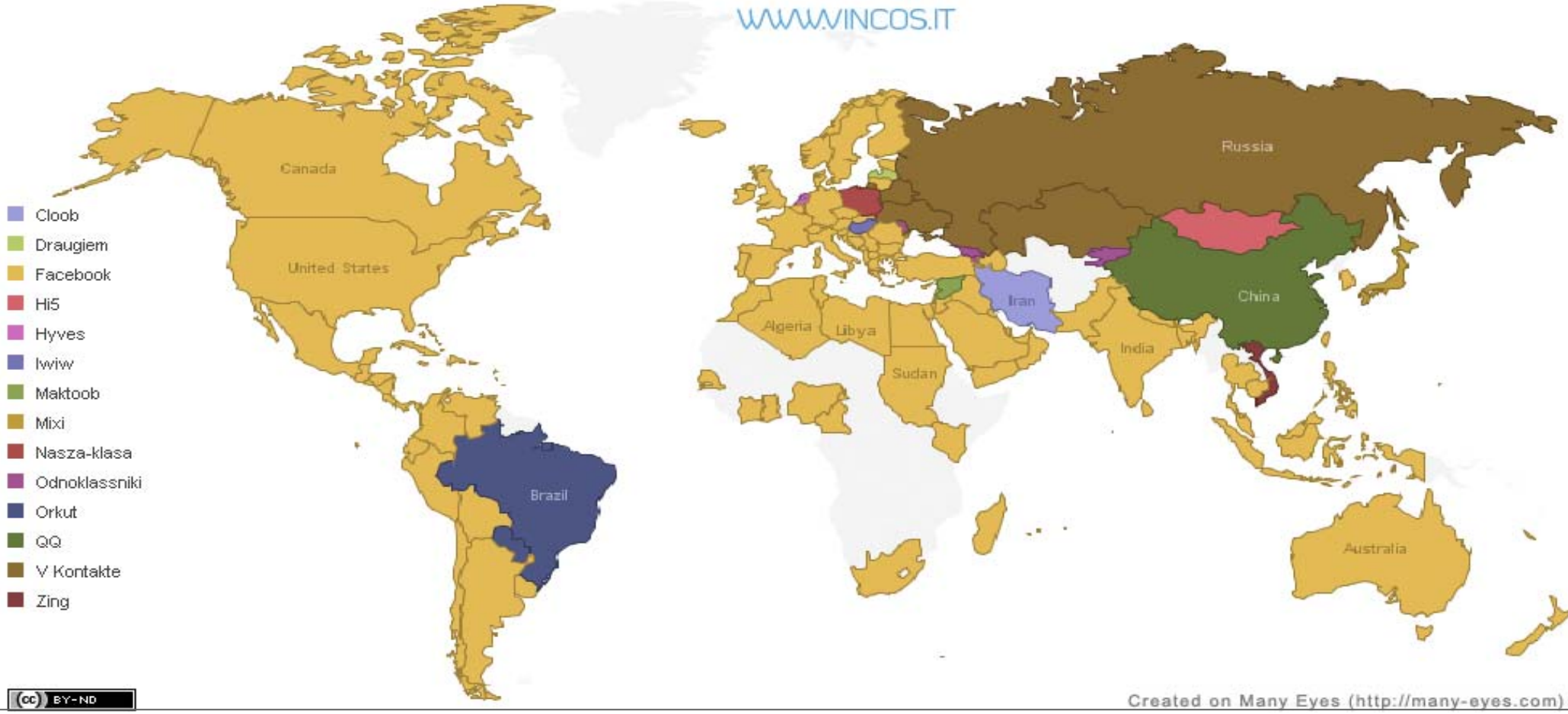
500 MILLIONS d'utilisateurs dans le monde.

19 MILLIONS d'utilisateurs en France.

(Facebook Statistics et Vincos Blog - Observatoire Facebook)

2 – LE PHÉNOMÈNE FACEBOOK

C’est le service de **réseau social** plus répandu au monde, que les utilisateurs préfèrent en Amérique, en Europe, en Afrique, en Inde, en Australie, …



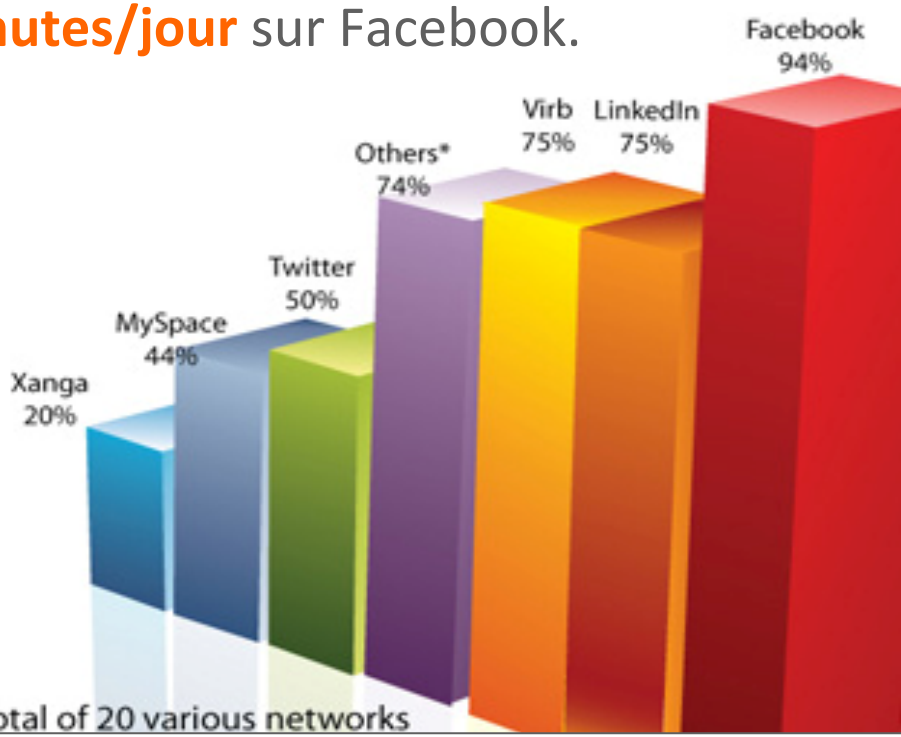
2 – LE PHÉNOMÈNE FACEBOOK

500 MILLIARDS.
Nombre de **minutes passées par mois** sur Facebook.

En moyenne, chaque utilisateur a **130 amis**, est connecté à **80 groupes et pages de communautés**, et passe **plus de 55 minutes/jour** sur Facebook.

Les **150 MILLIONS de membres** qui se connectent à Facebook depuis des **dispositifs mobiles** sont **deux fois plus actifs** que les autres utilisateurs du réseau.

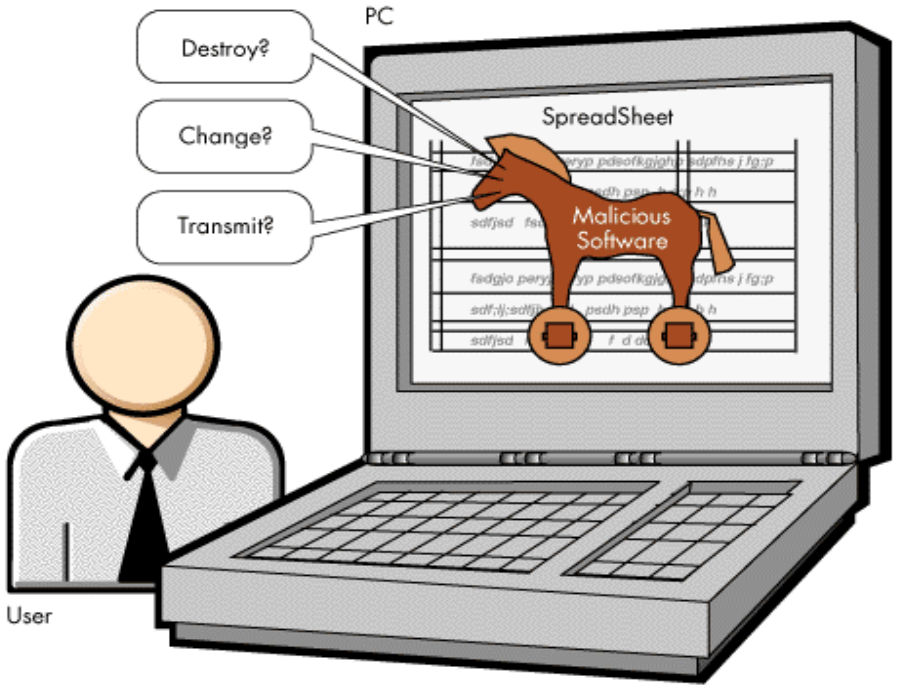
(Facebook Statistics)



3 – RISQUES ET MENACES : LOGICIELS MALVEILLANTS

Malware, forme abrégée de *"malicious software"*, indique un programme créé pour provoquer des dommages aux systèmes qu'il réussit à infecter.

Il y en a de différentes formes : virus, chevaux de Troie, espions, vers, rootkits, etc.



Ces logiciels malveillants peuvent provenir de **fichiers infectés**, pas seulement des exécutables mais également des documents (DOC, PDF, etc.).

En outre, un **navigateur vulnérable** peut exposer la machine au risque d'infections via l'exécution de codes malveillants présents sur certains sites, par le seul fait de naviguer sur leurs pages Web (même sans JavaScript ou sans Flash).

3 – RISQUES ET MENACES : VERS

Koobface, anagramme syllabique de Facebook, est l'exemple plus connu de **ver** capable d'infecter les **utilisateurs Windows de nombreux réseaux sociaux**.

Menace réelle depuis 2009, il agit en transmettant aux amis d'utilisateurs déjà infectés des messages contenant un lien vers une vidéo YouTube qui demande l'installation d'une mise à jour Adobe Flash. Or ce lien n'est autre qu'un *downloader* qui télécharge sur le système les composants malveillants de Koobface.

Défini par les experts comme **le plus grand Botnet du Web 2.0**, Koobface doit son "succès" à sa diffusion très rapide, vu la **confiance excessive** qu'ont les utilisateurs des réseaux sociaux envers les messages provenant de leurs amis.

3 – RISQUES ET MENACES : APPLICATIONS TIERCES

Sur Facebook (comme sur d'autres réseaux sociaux), quiconque peut développer des applications qui ont la caractéristique de **consentir l'accès à la base de données du réseau social**, de sorte qu'un utilisateur puisse transmettre ses contacts à tous les autres.

Or vu le **faible niveau des contrôles de sécurité** paramétrés par défaut, il peut être risqué d'utiliser des applications inconnues, susceptibles d'être des vecteurs potentiels de logiciels malveillants.

Mieux vaut donc vérifier attentivement les paramétrages de sécurité pour chaque application.

3 – RISQUES ET MENACES : SPAM

Le **spam**, difficilement endigué par les filtres des webmails, se décline à présent sous de nouvelles formes et frappe les utilisateurs des réseaux sociaux en envoyant des messages portant des liens qui pointent vers des sites internes ou externes, ou encore des invitations à s'inscrire à des groupes ou à accepter des demandes de contacts provenant d'inconnus.

Les réseaux sociaux mettent à la disposition des spammeurs une batterie d'outils : les **outils de recherche** permettent de sélectionner des segments démographiques donnés, et les **pages de fans et les groupes** d'envoyer des messages à tous les inscrits qui partagent les mêmes intérêts.

3 – RISQUES ET MENACES : SPAM & MALWARE

« 57% des utilisateurs déclarent avoir été la cible de spam provenant des sites "sociaux", soit une augmentation de 70% par rapport à l'année dernière.

36% révèlent avoir reçu des logiciels malveillants provenant des réseaux sociaux, en hausse de 69% par rapport à l'année dernière. »

Réseaux sociaux plus risqués :

1. Facebook : 60%

2. MySpace : 18%

3. Twitter : 17%

4. LinkedIn : 4%

(Sophos Threat Report 2010)

3 – RISQUES ET MENACES : PHISHING & WHALING

L'hameçonnage sur Internet est une déclinaison du **phishing** classique, destiné au vol de données bancaires ; aujourd'hui les tentatives ont pour but d'obtenir les donnés d'accès aux réseaux sociaux.

Un cas particulier est le **whaling** (*"pêche à la baleine"*) : attaque informatique visant à "craquer" des profils de haut niveau (administrateurs, dirigeants, etc.), en utilisant les informations diffusées par les victimes elles-mêmes sur les différents réseaux sociaux et les sites Web de leur propre entreprise, ou via des techniques d'**ingénierie sociale** tellement ciblées que les chances de réussir sont très élevées.

3 – RISQUES ET MENACES : VOL DE DONNÉES NUMÉRIQUES

Dans le cadre d'une expérience, BitDefender a collecté en ligne 250 000 données sensibles (identifiants, mots de passe, courriels) : 87% des comptes ainsi détectés sont encore opérationnels, tandis que dans 75% des cas le mot de passe est le même qui donne accès à la fois aux réseaux sociaux et au courriel.

« Les résultats préoccupants de cette expérience devraient faire prendre conscience aux utilisateurs que décider un mot de passe pour son compte email ou son réseau social devrait être un choix sérieux, tout comme celui d'ajouter une serrure de sûreté à sa maison. »

(Sabina Datcu, BitDefender E-Threat Analyst, à l'origine de l'expérience)

3 – RISQUES ET MENACES : USURPATION D'IDENTITÉ

La falsification d'identités et la création de faux profils ou de faux groupes est un phénomène de plus en plus répandu sur les réseaux sociaux.
Même si cela peut coûter cher : jusqu'à un an de réclusion pour le délit d'usurpation d'identité, auquel s'ajoute le délit de diffamation aggravée en cas de publication de paroles ou d'images offensives via Internet.

En Amérique, les faux profils atteignent 40% des nouveaux inscrits sur Facebook.

En Italie, ce pourcentage est de 20% du total.

(Cloudmark)

3 – RISQUES ET MENACES : FALSIFICATION D'IDENTITÉ

« Il suffit d'une photo, d'un nom et de quelques informations sur la vie d'une personne pour s'emparer de son identité en ligne. »

(Garant pour la protection des données personnelles – Réseau social : attention aux effets collatéraux)

Autre phénomène diffus : la création de faux profils qui ne **sont pas liés à des personnes réelles**, créés uniquement pour véhiculer des messages publicitaires ou malveillants via les liens sur la page.

Une photo « sympathique » peut permettre d' obtenir en peu de temps un grand nombre de contacts en donnant l'illusion d'un vrai profil.

3 – RISQUES ET MENACES : RESPECT DE LA VIE PRIVÉE

Les données personnelles, une fois qu'elles sont saisies sur les réseaux sociaux, **appartiennent à l'entreprise qui gère le site, conformément au contrat de licence d'utilisation accepté lors de l'inscription**, et peuvent être réélaborées et diffusées y compris des années plus tard.

Elles sont conservées même si vous décidez de quitter le réseau social, puisque **votre profil est désactivé mais il n'est pas effacé**.

Des problèmes au niveau du respect de la vie privée peuvent naître aussi en saisissant en ligne des informations sur vos connaissances (par exemple en les "*taguant*" sur une photo) : mieux vaut donc obtenir leur consentement avant, et éviter lorsqu'il s'agit de mineurs.

3 – RISQUES ET MENACES : DOMMAGES À L'IMAGE

Vu la rapidité à laquelle les informations se propagent sur les réseaux sociaux, les dommages à l'image de la personne ou de l'entreprise peuvent provoquer des préjudices importants.

Ils peuvent être **provoqués par des tiers** (cas de la diffusion de fausses infos sur la personne ou l'entreprise) ou **par soi-même** :

« L'énorme quantité d'informations personnelles publiées par les plus jeunes pourrait se retourner contre eux à l'avenir. Notamment lorsqu'ils chercheront un emploi. Dans certains cas, il pourrait même être nécessaire de changer d'identité numérique pour échapper à un cyber-passé gênant ou trop désinvolte. »

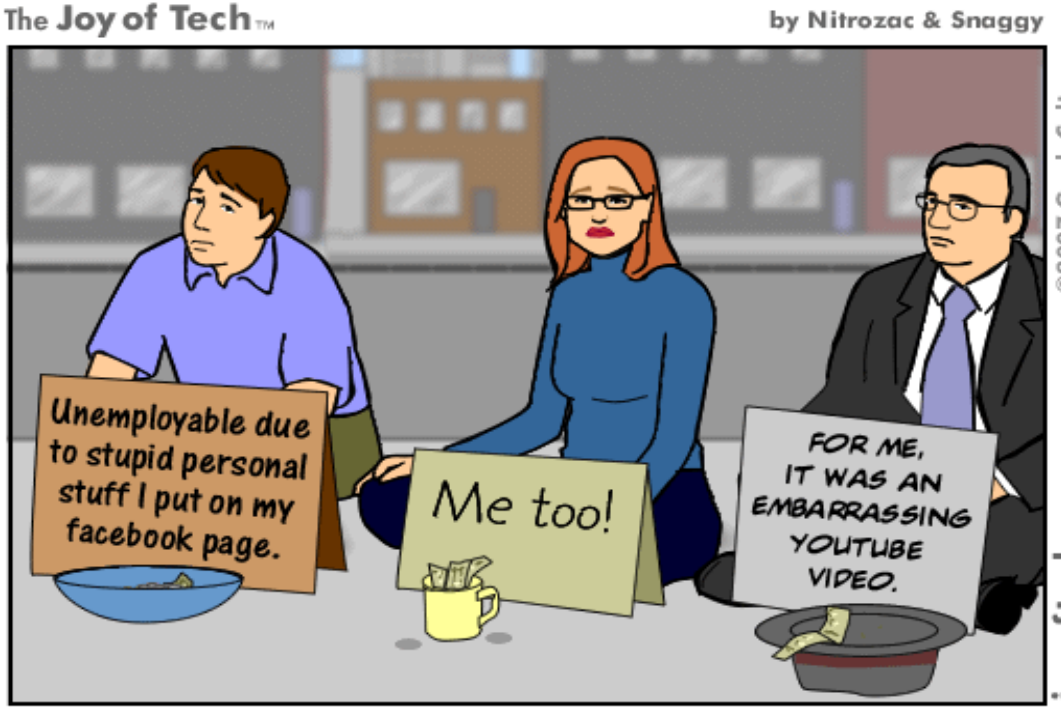
(Eric Schmidt, Ceo de Google)

3 – RISQUES ET MENACES : DOMMAGES À LA RÉPUTATION

95% d'entreprises utilisent LinkedIn pour trouver et attirer des collaborateurs.

59% utilisent Facebook, 42% Twitter.

*(What the F**K is social media now?)*



Signs of the social networking times.

3 – RISQUES ET MENACES : DONNÉES CONFIDENTIELLES

La perte de données confidentielles est un problème qui frappe surtout les **entreprises** et les administrations **gouvernementales** :

- Des photos ou des vidéos prises sur le lieu de travail peuvent involontairement révéler des informations délicates ;
- Le partage de données sur les voyages de travail peut dévoiler la localisation des clients ;
- Le partage (voulu ou non) de documents confidentiels peut provoquer de sérieuses difficultés à l'entreprise ou à l'organisation.

3 – RISQUES ET MENACES : BAISSES DE PRODUCTIVITÉ

D'après MyJobGroup, un portail anglais de recherche de travail, l'utilisation des réseaux sociaux au sein de l'entreprise a des répercussions négatives sur la productivité, ce qui provoque globalement un manque à gagner autour de 16,8 milliards d'euros, selon leurs estimations.

« 7% des membres de Facebook jouent en moyenne 68 minutes/jour au célèbre jeu interactif FarmVille. Mafia Wars, le deuxième jeu le plus connu, fait le bonheur de 5% des employés, avec une moyenne de 52 minutes par jour, et 4% des utilisateurs consacrent moyennement 36 minutes par jour à Café World, autre jeu populaire. »

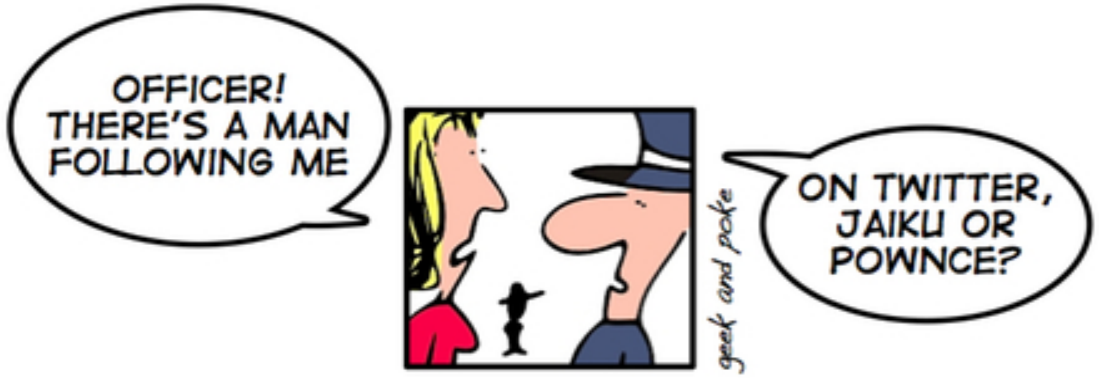
(Cisco Security Intelligence Operations)

3 – RISQUES ET MENACES : TROUBLES DU COMPORTEMENT

Les médias sociaux multiplient la possibilité de rencontrer des personnes victimes de **troubles** ou de développer soi-même des désordres du comportement et diverses formes de **dépendance**.

Selon une décision récente de la Cour de Cassation italienne, persécuter quelqu'un par le biais des réseaux sociaux peut être dénoncé et pénalement poursuivi pour harcèlement (délit de **stalking**).

3 – RISQUES ET MENACES DES MÉDIAS SOCIAUX



« Aujourd'hui le média social EST le média.
Et comme tous les médias, le risque est qu'il puisse être corrompu, pollué, trop commercial, trop politisé et trop puissant.
Il appartient à chacun de nous d'éviter que cela ne se produise. »

(Shiv Singh, Director Digital Engagement & Social Media PepsiCo. –
*What the F**K is social media now?)*

4 – LES PIÈGES PLUS RÉPANDUS

Symantec propose une liste des 5 pièges plus répandus sur les réseaux sociaux :

N° 1 Les URL cachées

Les URL abrégées, très fréquentes sur Twitter, sont utiles mais risquées car vous ne savez pas où elles vous conduiront : en cliquant dessus, vous pouvez accéder au site indiqué ou à un autre site qui installera toutes sortes de logiciels malveillants sur votre ordinateur.

Solution : **utiliser une protection en temps réel contre les logiciels espions et les virus, et ne cliquer que sur les liens postés par des personnes fiables.**

4 – LES PIÈGES PLUS RÉPANDUS

N° 2 L'hameçonnage (*phishing*)

Vous recevez un courriel contenant un lien qui pointe apparemment vers la page d'accueil de votre réseau social.

En réalité, la page où vous arrivez, semblable en tout et pour tout au site original, est créée par des cybercriminels pour collecter vos données de connexion.

Solution : **s'assurer que son système de sécurisation prévoie des fonctionnalités anti-phishing.**

Contrôler attentivement les URL de destination : ne jamais saisir vos données de connexion si vous n'êtes pas sûr que la page soit réellement celle de votre réseau social.

4 – LES PIÈGES PLUS RÉPANDUS

N° 3 Les frais cachés

L'un des innombrables tests qu'on vous propose en permanence sur les réseaux sociaux pourrait exiger la saisie de votre numéro de mobile où l'on vous communiquera les résultats.

Mais le « test gratuit et amusant » pourrait toutefois dissimuler l'envoi de SMS surtaxés ou l'abonnement à un service quelconque pour un coût "modique" de 9,95 € par mois ou autre...

Solution : **se méfier tout particulièrement des jeux diffusés sur les réseaux sociaux.**

4 – LES PIÈGES PLUS RÉPANDUS

N° 4 Les demandes d'argent

Imaginons qu'un ami en situation difficile parce qu'il dit avoir perdu son portefeuille nous contacte en nous demandant de lui envoyer de l'argent.

Seul problème : l'ami en question n'est au courant de rien et ignore tout du message : son ordinateur est infecté par un logiciel malveillant qui envoie de fausses demandes d'aide à tous ses contacts sur le réseau social.

Solution : **vérifier auprès de vos amis que les demandes d'argent sont réellement authentiques avant d'agir.**

4 – LES PIÈGES PLUS RÉPANDUS

N° 5 Les chaînes de lettres

Phénomène déjà connu dans le passé sous l'appellation de « chaîne de Saint-Antoine », il revient en force aujourd'hui grâce à l'expansion des réseaux sociaux, et en particulier Facebook, via les messages directs ou les groupes.

Par le biais de ces chaînes de lettres, les spammeurs réussissent à obtenir des contacts dont ils se serviront ensuite pour leurs campagnes.

Solution : **stopper la chaîne et avertir celle ou celui qui vous a transmis le message en bonne foi qu'il s'agit d'une arnaque.**

5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL

#1 Mots de passe

- Ne jamais utiliser le même mot de passe pour se connecter aux réseaux sociaux et à son courriel ou, pire encore, à son ordinateur ;
- Choisir un mot de passe **différent** pour chaque réseau social fréquenté ;
- Préférer des mots de passe **complexes** (au moins 8 caractères, lettres et chiffres) ;
- Ne jamais saisir dans ses mots de passe des termes facilement identifiables en ligne (date de naissance, prénom des enfants ou du conjoint, …) ;
- Changer souvent de mot de passe.

5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL

#2 Sécurité

- Utiliser un **antivirus** sérieux (certains bons produits sont également gratuits) et l'actualiser tous les jours ;
- Faire une analyse antivirus de tout le système au moins une fois par semaine ;

- Utiliser un **anti-malware** distinct de l'antivirus ;
- Éliminer régulièrement les **cookies** et le cache de l'historique des navigateurs utilisés (il y a des nettoyeurs ad hoc) ;
- Se déconnecter des réseaux sociaux après chaque session ;
- Toujours actualiser le **navigateur** à la version plus récente disponible.

5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL

#3 Respect de la vie privée

- Il est fondamental de limiter le plus possible les **informations de base** accessibles à tous, et de permettre la vision de son profil intégral uniquement aux amis ;
- Mieux vaut personnaliser les options de **partage sur Facebook** et n'autoriser que les seuls amis à voir nos mises à jour, tandis que les photos ou les vidéos où nous sommes tagués ne devraient être visibles qu'à nous-même, pour éviter la diffusion éventuelle de choses embarassantes ;
- Pour ce qui concerne les **applications**, il est fondamental de paramétrer non seulement qui peut voir nos activités, mais également quelles sont nos informations disponibles aux applications de nos amis (pour tout dire, "aucune information" serait préférable).

5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL

#4 Discrétion

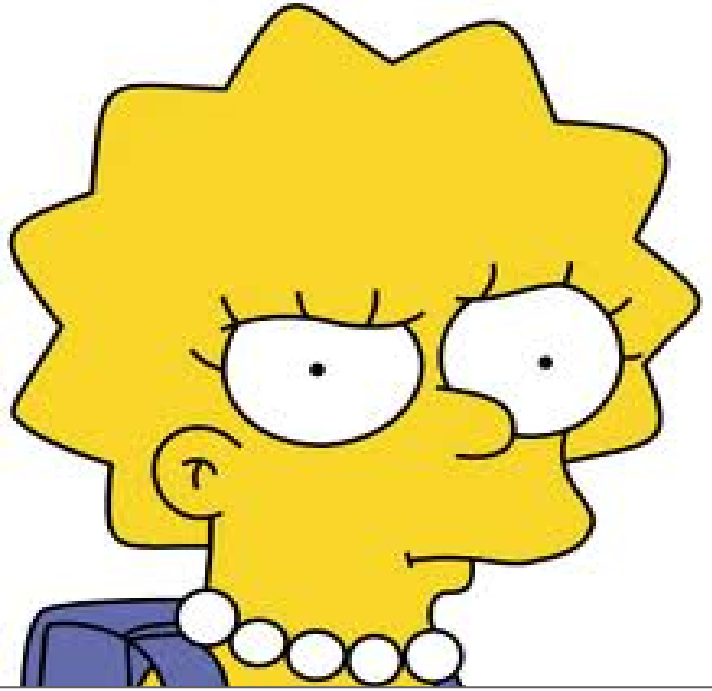
- Ne jamais saisir en ligne de données susceptibles de vous exposer à des usurpations d'identité, au spam, au *stalking*, etc. : adresses, numéros de téléphone, date de naissance, informations confidentielles sur votre activité professionnelle ou votre famille.
- D'une manière générale, ne pas divulguer d'informations que pourraient utiliser des personnages sans scrupules.
- Ne jamais **rien poster que vous pourriez regretter ensuite**, comme des obscénités ou des insultes : les contenus des réseaux sociaux sont indexés par les moteurs de recherche et peuvent rester visibles à tous pendant des années…

5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL

#5 Scepticisme

- Les réseaux sociaux contiennent les unes à côté des autres des informations utiles, erronées, tendancieuses ou délibérément fausses.

- Tout ce que nous lisons sur le Web doit être pesé avec une bonne dose de scepticisme ; il faut apprendre à discerner le vrai du faux, du mensonge, de l'ignorance et de la stupidité, en vérifiant toujours ses sources.



5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL

#6 Circonspection

- Ne jamais dévoiler à des inconnus d'infos personnelles, professionnelles ou financières ;

- Mieux vaut refuser les demandes de contact provenant d'inconnus, à moins d'avoir la certitude qu'il y a bien une personne réelle derrière le profil ;
- Se méfier des liens étranges ou des messages improbables postés sur les pages des autres, surtout lorsqu'il s'agit d'inconnus ;
- Contrôler soigneusement la fiabilité des demandes d'envoi d'argent, quand bien même elles proviennent de vos "amis".

5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL

#7 Sérieux

- Quels que soient les contenus saisis en ligne ou les groupes que l'on fréquente, toujours s'assurer que notre comportement en ligne nous représente au mieux, vu qu'il est potentiellement sous le regard de quiconque.

- Il est toujours préférable d'avoir une attitude sérieuse et correcte, de distinguer l'humorisme et l'esprit des banalités, de la stupidité et de la mauvaise éducation.

5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL

#8 Prudence

- Décider de ne pas créer son profil sur Facebook ou sur d'autres réseaux sociaux pour ne pas s'exposer reste malheureusement insuffisant.

- On perd ainsi totalement le contrôle sur tout ce que les autres disent de nous, sur les tags nous concernant susceptibles d'étiqueter des photos ou sur les faux profils éventuellement créés à notre nom.

- Mieux vaut se créer un compte et l'utiliser avec le plus grand soin pour garder le contrôle des "rumeurs" et maîtriser son image.

5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL

#9 Conscientisation

- Probablement le conseil le plus important.
- Toujours être conscients des risques et des menaces auxquels l'utilisation des médias sociaux nous expose, sans renoncer pour autant à bénéficier de leurs avantages évidents.
- Les réseaux sociaux ne sont pas des jouets, au contraire : ce sont des outils extrêmement puissants, à utiliser avec attention et bon sens, pour apprendre à en tirer le meilleur.

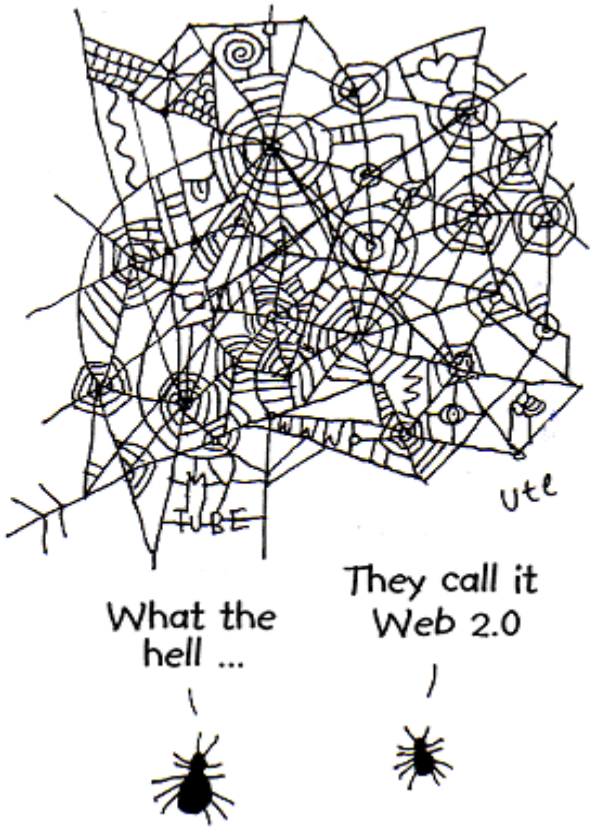
5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL

10 conseils pour une utilisation sécurisée des médias sociaux en milieu de travail

1. Augmenter la prise de conscience des collaborateurs
2. Élaborer des poliques et des processus internes en la matière
3. Appliquer les règles de façon systématique
4. Bloquer les sites infectés
5. S'équiper de pare-feux de dernière génération
6. Gérer l'accès aux applications de l'entreprise
7. Se protéger contre les vulnérabilités logicielles
8. Défendre le réseau Intranet et les données "maison"
9. Inclure aux politiques de sécurité les dispositifs mobiles
10. Utiliser une gestion centralisée de la sécurité

(*Stonesoft : 10 conseils pour utiliser les médias sociaux en toute sécurité*)

5 – CONSEILS POUR UN USAGE SÛR ET AVISÉ DU WEB SOCIAL



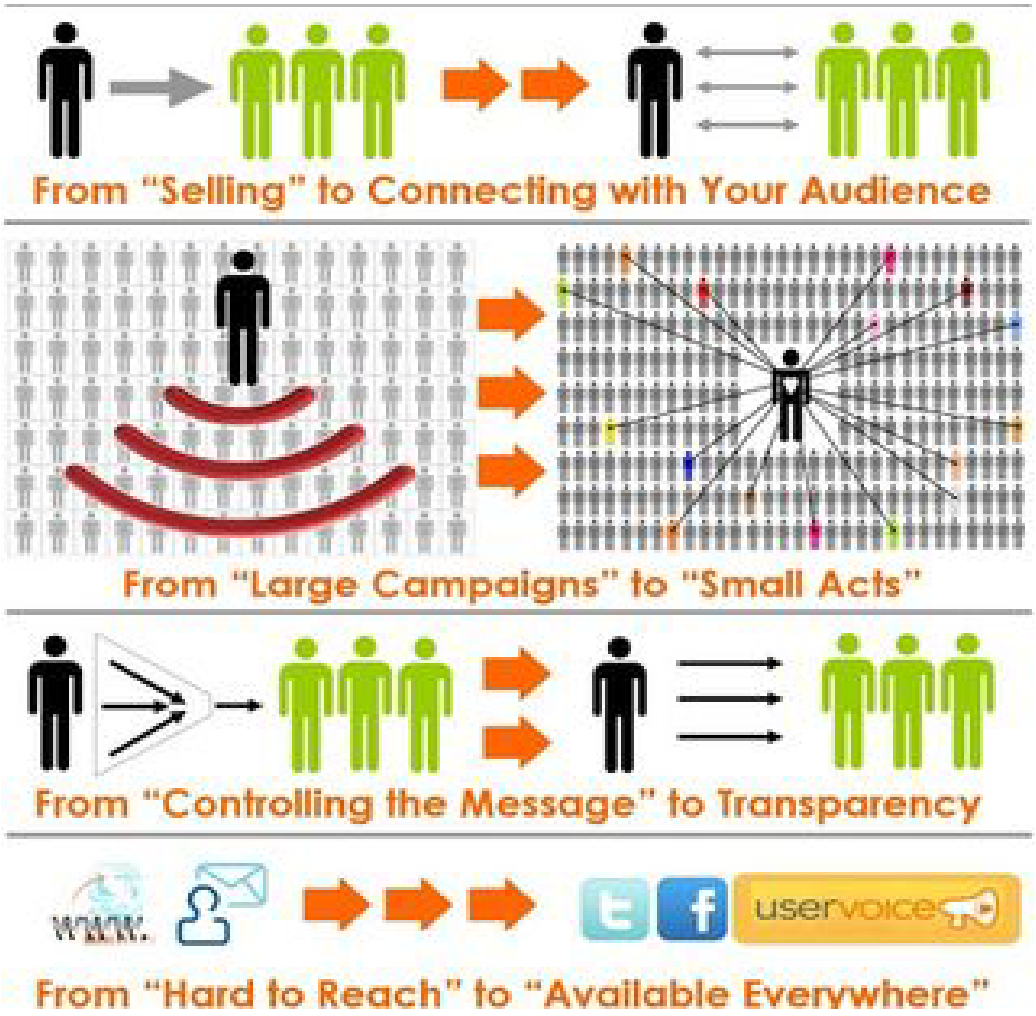
« L'utilisation grandissante des médias sociaux comporte des risques supplémentaires pour les réseaux de l'entreprise. L'adoption d'outils pour protéger les réseaux internes est devenue une priorité. Pour autant, grâce à une bonne stratégie de sécurité qui conjugue les cours de formation continue pour le personnel et les technologies plus modernes, les organisations de toute taille peuvent aujourd'hui bénéficier des avantages des réseaux sociaux. »

(Emilio Turani, Manager Pays de Stonesoft Italia, pour la Suisse italienne, la Grèce et la Turquie)

6 – CONCLUSIONS

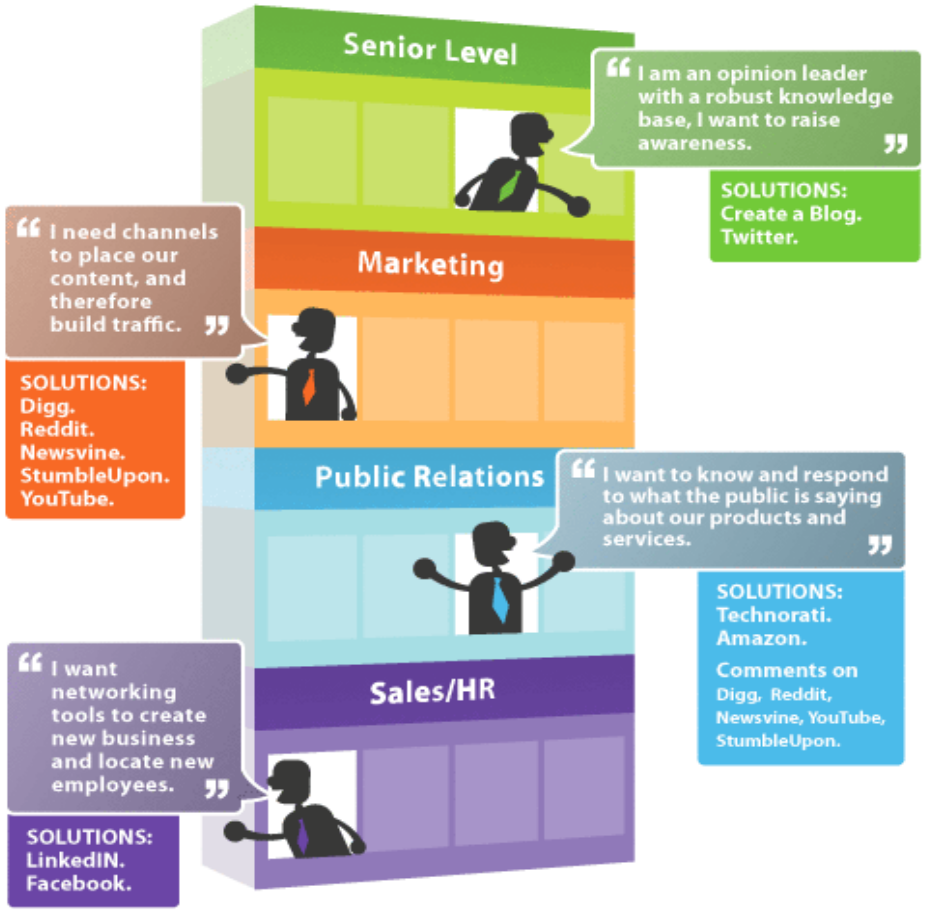
Le Web 2.0 et l'avènement des nouveaux médias sociaux font **évoluer la communication et les modes de travail**.

Un phénomène tellement massif que nul ne saurait plus l'ignorer : il doit être **compris** dans ses différents aspects, dont les **risques** qu'il implique, et **géré** pour en garantir l'utilisation en toute **sécurité**.



6 – CONCLUSIONS

Les nouveaux médias sont devenus des outils de travail et
de relations professionnelles.



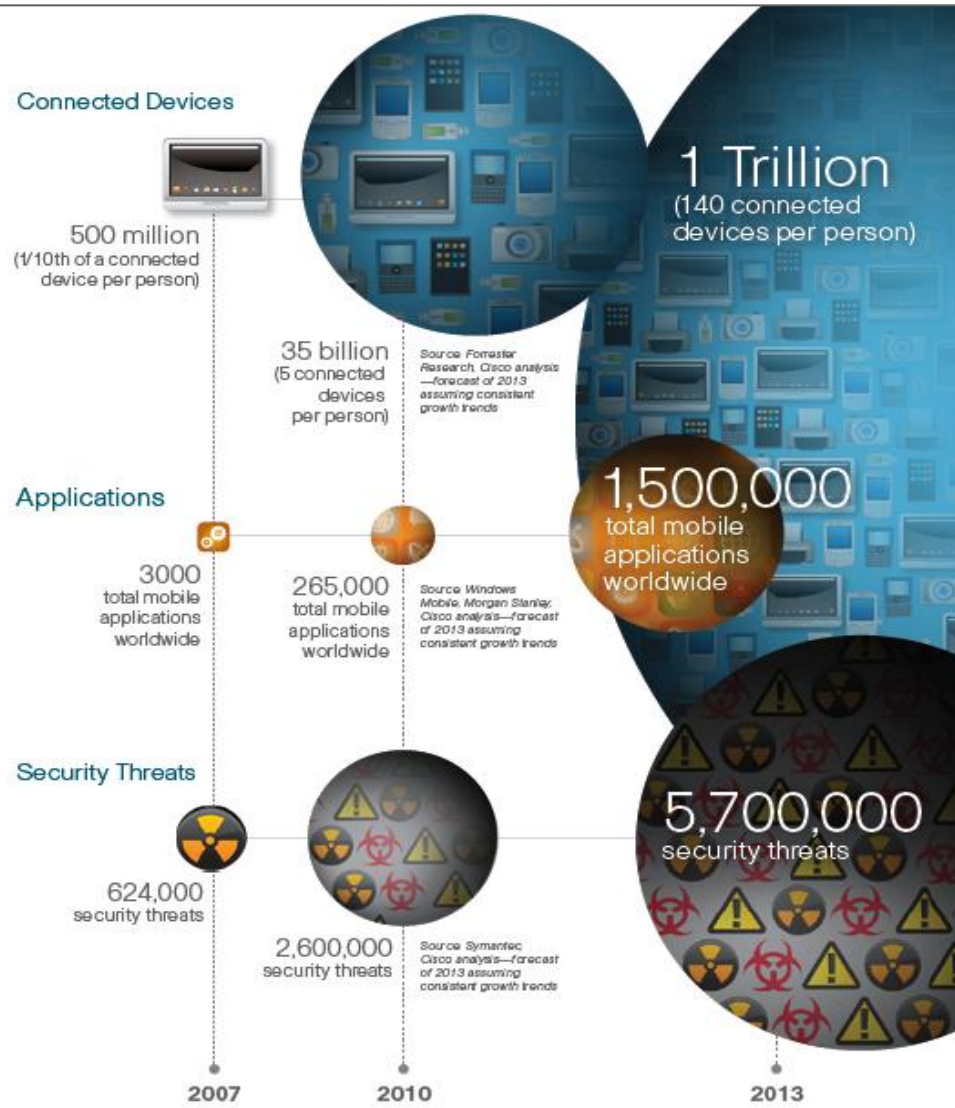
« Nous sommes dans une phase de transition où la globalisation des systèmes est en train de redéfinir les relations sociales et tous les niveaux de l'organisation sociale, y compris dans les entreprises, qui sont en ce moment peu ou pas du tout préparées pour endiguer les risques découlant des nouveaux usages qu'autorisent les outils en ligne, et ne réussissent pas à transformer cette opportunité en avantage compétitif. »

(Ugo Guidolin, Professeur de Communication multimédia, Université de Padoue, Consultant pour les nouveaux médias)

6 – CONCLUSIONS

La diffusion des médias sociaux et l'impact des nouvelles technologies sur nos vies implique un **accroissement exponentiel des dispositifs connectés**, d'où une hausse correspondante des risques en termes de sécurité, et en particulier en milieu mobile.

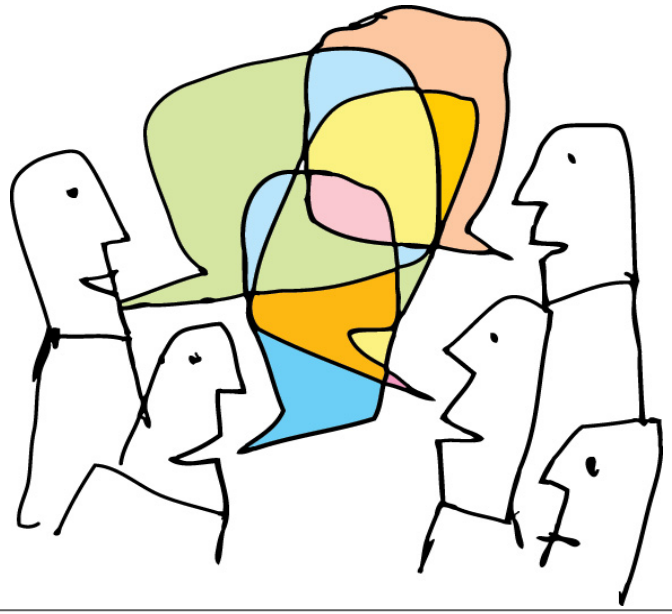
Les problématiques inhérentes à la sécurité des médias sciaux doivent donc être affrontées et résolues dès à présent, autant dans le cadre privé qu'au sein des entreprises, puisque désormais la croissance du phénomène ne peut plus être stoppée.



6 – CONCLUSIONS

« Aujourd'hui, une entreprise qui ferme les portes aux nouvelles opportunités qu'offre le Web 2.0 risque sérieusement de perdre un gros avantage compétitif »

(Ugo Guidolin, Professeur de Communication multimédia, Université de Padoue, Consultant pour les nouveaux médias)



La sécurité des médias sociaux n'est certainement pas une question que l'on résoudra en tenant compte **uniquement de l'aspect technologique**.

Aucun outil informatique au monde, pour autant qu'il soit moderne et perfectionné, n'est capable de sécuriser les risques découlant de négligences superficielles, de lacunes organisationnelles et du maque de prise de conscience des utilisateurs.

6 – CONCLUSIONS

La sécurité des médias sociaux s'obtient autant en accroissant le niveau de **prise de conscience des utilisateurs** qu'en les faisant devenir **partie intégrante de la *security chain***, c'est-à-dire en les impliquant activement dans les contre-mesures et en les rendant **responsables** en cas d'incidents.

Par conséquent les solutions sont à la fois technologiques, organisationnelles, légales et culturelles.

« Si nous voulons rehausser le niveau de la sécurité informatique de manière significative, nous devons dépasser l'idée obsolète que l'utilisateur final est un sujet obtus et inerte, passif au sein de son organisation. Car les problèmes ne naissent pas seulement à cause du manque de prise de conscience et de formation, mais surtout à cause du manque d'implication et de responsabilité. »

(Andrea Zapparoli Manzoni, CEO iDialoghi)

6 – CONCLUSIONS

« Les trois voies qui conduisent à la sagesse sont la conscience, la conscience et la conscience. »

(Bouddha)

« Merci ! »

iDIALOGHI

ICT Security & Consulting

web http://www.idialoghi.com

courriel info@idialoghi.com

skype idialoghi

[traduction info@translation2.com **]**