

Université de Montréal

**PROTECT\_U: Un système communautaire pour la protection des usagers de Facebook**

Par

Ala Eddine Gandouz

Département d'informatique et de recherche opérationnelle

Faculté des arts et des sciences

Mémoire présenté à la Faculté des arts et sciences

en vue de l'obtention du grade de Maitrise ès sciences (M.Sc.)

en Informatique

Aout, 2012

Copyright, Ala Eddine Gandouz, 2012

Université de Montréal

**PROTECT\_U: Un système communautaire pour la protection des  
usagers de Facebook**

Par

Ala Eddine Gandouz

Département d'informatique et de recherche opérationnelle

Faculté des arts et des sciences

Membres de jury :

Abdelhakim Hafid, président

Esma Aïmeur, directrice de recherche

Louis Salvail, membre de jury

Aout, 2012

## Résumé

Chaque année, le nombre d'utilisateurs des réseaux sociaux augmente à une très grande vitesse. Des milliers de comptes usagés incluant des données privées sont créés quotidiennement. Un nombre incalculable de données privées et d'informations sensibles sont ainsi lues et partagées par les différents comptes. Ceci met en péril la vie privée et la sécurité de beaucoup d'utilisateurs de ces réseaux sociaux. Il est donc crucial de sensibiliser ces utilisateurs aux dangers potentiels qui les guettent.

Nous présentons *Protect\_U* (*Hélou, Gandouz et al. 2012*), un système de protection de la vie privée des utilisateurs de Facebook. *Protect\_U* analyse le contenu des profils des utilisateurs et les classes selon quatre niveaux de risque : *Low risk, medium risk, risky and critical*. Il propose ensuite des recommandations personnalisées pour leur permettre de rendre leurs comptes plus sécuritaires. Pour ce faire, il fait appel à deux modèles de protection : local et communautaire. Le premier utilise les données personnelles de l'utilisateur afin de lui proposer des recommandations et le second recherche ses amis de confiance pour les inciter à participer à l'amélioration de la sécurité de son propre compte

**Mots clés:** Facebook, vie privée, profil utilisateur, sites de réseaux sociaux, système de recommandation, filtre communautaire, classification.

## Abstract

Social networking sites have experienced a steady and dramatic increase in the number of users over the past several years. Thousands of user accounts, each including a significant amount of private data, are created daily. As such, an almost countless amount of sensitive and private information is read and shared across the various accounts. This jeopardizes the privacy and safety of many social network users and mandates the need to increase the users' awareness about the potential hazards they are exposed to on these sites.

We introduce Protect\_U (Hélou, Gandouz et al. 2012), a privacy protection system for Facebook users. Protect\_U analyzes the content of user profiles and ranks them according to four risk levels: Low Risk, Medium Risk, Risky and Critical. The system then suggests personalized recommendations designed to allow users to increase the safety of their accounts. In order to achieve this, Protect\_U draws upon both the local and community-based protection models. The first model uses a Facebook user's personal data in order to suggest recommendations, and the second seeks out the user's most trustworthy friends to encourage them to help improve the safety of his/her account.

**Keywords:** Facebook, online privacy, user-profile, social network sites, recommender system, community filter, classification.

# Table des matières

Résumé .....	3
Abstract.....	4
Table des matières.....	5
Remerciements .....	7
Chapitre 1 : Introduction.....	8
Chapitre 2 : Les réseaux sociaux .....	10
2.1    Les bases des réseaux sociaux .....	11
2.2    L'histoire des réseaux sociaux.....	12
2.3    L'utilisation des réseaux sociaux.....	15
2.4    Pourquoi utilise-t-on les réseaux sociaux .....	20
Chapitre 3 : Problématique.....	26
3.1    Risques encourus .....	26
3.2    Techniques de fraudes utilisées.....	28
Chapitre 4 : Les systèmes de protections de la vie privée .....	40
4.1    Survol .....	40
4.2    Études sur les risques.....	44
4.3    Solutions proposées.....	48
Chapitre 5 : Conception et méthodologie .....	53
5.1    Module de classification.....	55
5.2    Module de recommandation .....	59
Chapitre 6 : Implémentation et validation.....	65
6.1    Module de classification .....	65
6.2    Module de recommandation .....	68
Chapitre 7 : Conclusion .....	73
Références .....	75

FIGURE 1: LES SIX DEGRES DE SEPARATION .....	12
FIGURE 2: LE TOP 10 DES RESEAUX SOCIAUX PAR TAUX DE TRAFIC .....	16
FIGURE 3: CARTE DU MONDE DES RESEAUX SOCIAUX DE 2011 .....	17
FIGURE 4: CARTE DU MONDE DES RESEAUX SOCIAUX DE 2007 .....	18
FIGURE 5: L'UTILISATION DES RESEAUX SOCIAUX PAR TRANCHE D'AGE ENTRE 2005 ET 2011 .....	19
FIGURE 6: COMPARAISON ENTRE LES SEXES DANS LES RESEAUX SOCIAUX EN 2010 .....	20
FIGURE 7: POUR QUELLE RAISON LES INTERNAUTES UTILISENT LES RESEAUX SOCIAUX.....	21
FIGURE 8: PROFIL DE BARACK OBAMA SUR FACEBOOK .....	22
FIGURE 9: RECHERCHE DE CLASSE SUIVANT L'ANNÉE DE GRADUATION SUR CLASSMATES.COM .....	23
FIGURE 10: GROUPE DE PHILATÉLIE SUR FACEBOOK.....	24
FIGURE 11: ÉVÈNEMENT ORGANISÉ SUR LINKEDIN.....	24
FIGURE 12: OFFRE D'EMPLOI SUR LINKEDIN .....	25
FIGURE 13: SOURCES DES SPAMS EN JUIN 2012 .....	30
FIGURE 14: SPAMS PAR CATEGORIES.....	31
FIGURE 15: LE TOP 10 DES ORGANISATIONS VISEES PAR LES ATTAQUES DE PHISHING EN JUIN 2011.....	35
FIGURE 16: LE NOMBRE DE VICTIMES DE VOL D'IDENTITE .....	38
FIGURE 17: POURCENTAGE D'ACCEPTATION DES DEMANDES D'AJOUT.....	45
FIGURE 18 : IMPRIME ECRAN DE QUESTIONS POSEES A L'UTILISATEUR.....	49
FIGURE 19: IMPRIME ECRAN D'UNE QUESTION DETAILLEE POSEE A L'UTILISATEUR .....	49
FIGURE 20: AUDIENCE VIEW INTERFACE .....	51
FIGURE 21 : ARCHITECTURE DE PROTECT_U.....	55
FIGURE 22 : QUESTION LIEE AUX PROFILS MOYENNEMENT RISQUES.....	56
FIGURE 23 : QUESTION LIEE AUX PROFILS RISQUES.....	56
FIGURE 24 : QUESTION LIEE AUX PROFILS CRITIQUES .....	56
FIGURE 25 : EXEMPLE D'EXTRACTION DE SCENARIOS .....	58
FIGURE 26. RECOMMANDATION MODULE.....	59
FIGURE 27 : L'ENSEMBLE DES REGLES EXTRAITES DE L'ARBRE DE DECISION .....	66
FIGURE 28. LE QUESTIONNAIRE DE VALIDATION .....	68
FIGURE 29 : LE POURCENTAGE DES PARTICIPANTS PAR NIVEAU DE RISQUE .....	69
FIGURE 30 : PRECISION DE LA SELECTION DES AMIS DE CONFIANCES PAR NIVEAU DE RISQUE .....	70
FIGURE 31 : PROFILE TROUVE VS PROFILE PREDIT.....	70
FIGURE 32 : POURCENTAGE DES RECOMMANDATIONS JUGEES UTILES PAR UTILISATEUR, ET POURCENTAGE DES UTILISATEURS QUI COMPTENT APPLIQUER CES RECOMMANDATIONS.....	71
FIGURE 33 : POURCENTAGE DES UTILISATEURS QUI SONT PRETS A CHANGER LEUR COMPORTEMENT PAR NIVEAU DE RISQUE .	72

## Remerciements

Je voudrai tout d'abord adresser mes remerciements les plus sincères à ma directrice de recherche, professeure Esma Aïmeur pour m'avoir dirigé et soutenu tout au long de ce projet, surtout dans les moments difficiles. Elle m'a facilité la tâche en fournissant de précieux conseils et a toujours été disponible pour moi.

Je voudrai remercier aussi les membres du jury d'avoir accepté d'évaluer mon travail.

Mes remerciements vont également à tous les membres du laboratoire Heron, spécialement à Charles Helou pour toute les discussions enrichissantes que nous avons eues au cours de nos rencontres.

Je tiens aussi à remercier ma femme Meriam, pour son soutien moral, sa patience et son encouragement constant et mes parents qui m'ont toujours apporté soutien et réconfort.

Enfin, un remerciement spécial à mes amis qui m'ont aidé de loin ou de près pour l'accomplissement de cet ouvrage, en particulier, ceux qui m'ont offert de leur précieux temps pour lire et réviser ce mémoire.

# Chapitre 1 : Introduction

Les réseaux sociaux permettent aux utilisateurs de rester en contact avec des amis, de discuter et de partager avec eux des informations. Ils leurs fournissent des outils d'interaction et de communication qui leurs permettent d'agrandir leurs réseaux d'amis et d'interagir via des applications tierces.

Chaque jour des milliers, de nouveaux comptes sont créés (300,000 nouveaux utilisateurs par jour se sont inscrits sur *Twitter* en 2011(Hussey 2011)), et des millions de données privées de tout genre sont partagées (250 millions de photos sont publiées chaque jour sur *Facebook* en 2011<sup>1</sup>).

Bien que la fonction première des réseaux sociaux reste l'interaction entre les internautes et la découverte de nouveaux amis, l'ignorance et l'insouciance de certains utilisateurs face à la publication d'informations personnelles sur leurs comptes peuvent mettre leur vie privée en danger. En effet plusieurs informations sensibles peuvent être facilement accessibles par les amis, mais aussi par des inconnus. Très souvent, les internautes ne sont pas conscients que leurs profils peuvent être consultés par n'importe qui. Ils affichent régulièrement beaucoup de détails sur leur vie privée dans leurs comptes croyant qu'ils se trouvent dans un espace virtuel et qu'ils sont protégés. Ce phénomène est d'autant plus favorisé par les sites de réseaux sociaux qui mettent à la disposition des utilisateurs un espace de collecte d'informations très détaillé qui comporte beaucoup de leurs informations personnelles. Dans certains cas, ils les obligent à saisir des informations très confidentielles (*Facebook* oblige les nouveaux utilisateurs à saisir leurs *dates de naissance* et leurs *sexes*, il oblige aussi ceux qui veulent créer des applications sur sa plateforme à donner un numéro de téléphone valide ou bien un numéro de carte de crédit<sup>2</sup>). C'est pourquoi la sensibilisation de ces internautes aux dangers des réseaux sociaux est primordiale.

---

<sup>1</sup> <https://www.facebook.com/press/info.php?statistics>

<sup>2</sup> <https://www.facebook.com/help/search/?q=verify+account>

Nous proposons dans ce qui suit un système de protection de la vie privée des utilisateurs de Facebook basé sur une approche communautaire. Nous commençons par présenter les réseaux sociaux dans la section 1, leurs spécificités et les différents aspects sur lesquels ils sont basés. Dans la section 2, nous présentons la problématique et les principaux dangers auxquels sont confrontés actuellement les internautes. La section 3 présente d'importants travaux de recherche qui ont traité ce sujet. La section 4 expose la méthodologie appliquée ainsi que les différentes techniques utilisées. Dans la section 5, nous présentons l'implémentation du système ainsi que et les résultats obtenus lors de la validation. Nous concluons avec la section 6.

## Chapitre 2 : Les réseaux sociaux

Fogel et Nehmad (Fogel and Nehmad 2009) ont présenté les réseaux sociaux comme un espace social sur internet utilisé pour faciliter la communication, la collaboration et le partage des informations entre les personnes.

Il repose sur trois principes essentiels :

- Le profil du membre, il peut insérer diverses informations personnelles, des photos, des news, des articles, des liens vers d'autres sites...
- La possibilité d'ajouter d'autres membres à une liste de contacts et de créer des sous listes selon un thème bien précis (collègues de travail, copains de lycée...)
- L'interaction entre les abonnés : envoi de messages, marquage de photos, discussion en ligne...

Le réseau social permet à des personnes ou des organismes de modéliser et d'administrer leurs listes de contacts en ligne.

Les utilisateurs peuvent créer leurs profils, ajouter des événements, ajouter des informations personnelles telles que l'opinion politique et la religion, ils peuvent aussi ajouter des amis dans leurs contacts ou restreindre la visibilité de certaines informations pour certains contacts.

Le principe de visibilité et la restriction d'information est très important dans les réseaux sociaux, il permet aux membres et aux groupes de contrôler qui peut accéder, afficher des informations ou modifier leurs profils. Et ceci en spécifiant différents niveaux de contrôle qui varient suivant des besoins bien spécifiques :

- Protéger les informations privées et ne pas donner l'accès qu'à des personnes bien spécifiques.

- Restreindre la visibilité des informations personnelles à une liste de contacts ou à un groupe particulier.
- Mettre les informations personnelles publiques pour que tout le monde même ceux qui ne sont pas dans les contacts de l'utilisateur puisse y accéder.

À travers ces niveaux de contrôle et de permissions, les utilisateurs peuvent organiser leurs contacts, leurs groupes ou la façon dont ils sont accessibles pour le public.

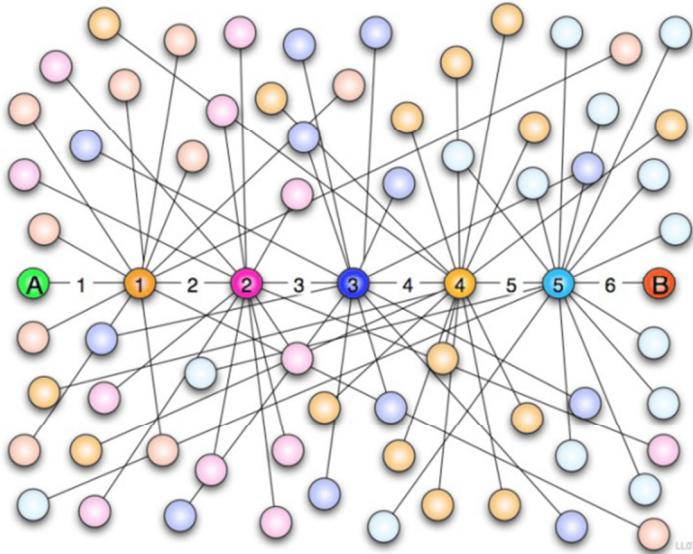
## 2.1 Les bases des réseaux sociaux

La théorie des réseaux sociaux est un domaine très actif dans le milieu universitaire et plusieurs études ont été faites sur le sujet. Nous avons extrait les études les plus importantes sur le sujet et qui ont été la base des réseaux sociaux.

### 2.1.1 Les degrés de séparation

Les degrés de séparations se basent sur le principe que chacun d'entre nous peut être lié à n'importe quelle personne au monde à travers six personnes intermédiaires au maximum. Cette théorie a été étudiée par des chercheurs à Microsoft (Horvitz et Leskovec (Leskovec and Horvitz 2008)) sur 180 millions d'utilisateurs de Live Messenger.

L'étude a révélé qu'il faut en moyenne créer des liens avec 6.6 contacts avant de pouvoir parler à n'importe qui dans le monde qui ne figure pas dans sa liste de contacts.



**Figure 1: Les six degrés de séparation**

### 2.1.2 Règle de 150 (Nombre de Dunbar)

Cette règle fixée par Hernando et al. (Hernando, Villuendas et al. 2010) soutient que la taille d'un réseau social est limitée à environ 150 membres, donc c'est le nombre d'amis qu'une personne peut avoir et entretenir une relation stable avec elle.

Plusieurs théories tournent autour de ce nombre, il peut être dû à une certaine limite d'une personne à reconnaître les membres et à leur donner une confiance mutuelle au-delà de cette limite.

### 2.1.3 La loi de Reed

La loi de Reed est définie par Cushman (Cushman 2010) comme suit : « Les réseaux qui encouragent la construction de groupes qui communiquent créent une valeur qui croît de façon exponentielle avec la taille du réseau ».

## 2.2 L'histoire des réseaux sociaux

Boyard et Elyson (Boyd and Ellison 2007) ont étudié toute l'histoire des réseaux sociaux. On peut extraire trois phases déterminantes :

## 2.2.1 Le début des réseaux sociaux et les premiers principes

Le premier réseau social est lancé en 1997. C'était *SixDegrees.com*. Il permet déjà à l'utilisateur de créer un profil et lister ses amis. Ce n'est pas la première fois qu'on utilise le concept de liste d'amis, cela existe depuis longtemps dans les sites de rencontres tels que *icq.com* ou *aim.com* où on peut ajouter des amis avec leurs noms, mais ce qui a changé c'est que la liste d'amis d'un utilisateur est devenue visible à tous ses amis aussi.

*SixDegrees* se décrit comme un outil pour aider les gens à se connecter et à envoyer des messages à leurs amis. Et bien qu'il a attiré des millions d'utilisateurs, il n'a pas pu se développer à cause des utilisateurs qui n'étaient pas habitués à ce genre de services et qui se limitaient à accepter seulement ceux qu'ils connaissaient. Il n'a pas pu continuer à fournir ses services et due fermer en 2000.

De 1997 à 2001, plusieurs sites de réseaux sociaux sont apparus, combinant les profils et les listes d'amis. On peut citer par exemple *AsianAvenue*, *MiGente* ou encore *BlackPlanet*. On note aussi l'apparition de nouveaux concepts tels que la possibilité de voir le profil d'un utilisateur sans l'accepter comme ami, le livre d'or... On a remarqué aussi que plusieurs anciens sites se sont remodelés pour suivre la mode des réseaux sociaux, dont *LiveJournal*, le Korean *Cyworld* ou encore le Suédois *LunarStorm*.

## 2.2.2 Maturation et diversification de la concurrence

En 2001, une nouvelle vague de réseaux sociaux qui est les réseaux professionnels a commencé avec *Ryse.com*. *Ryse* a commencé comme un réseau social entre amis, puis il a attiré des membres de la San Francisco Business and Technology incluant des entrepreneurs et des investisseurs responsables d'autres réseaux sociaux professionnels dont *Tribe.net*, *Friendster* et *LinkedIn*. Tous ces membres croyaient qu'ils pourraient se soutenir mutuellement sans concurrence. Mais à la fin, *Ryse* n'a pas pu attirer assez d'utilisateurs, *Friendster* s'est orienté vers les réseaux sociaux d'amis et seul *LinkedIn* est devenu un puissant service professionnel. Toutefois, *Friendster* est considéré comme le premier réseau social qui regroupe la plupart des

fonctionnalités existantes dans ses concurrents actuels et le numéro un des sites de réseaux sociaux jusqu'en 2004 où il a été dépassé par *MySpace*.

Depuis 2003, plusieurs réseaux sociaux ont vu le jour. La plupart ont essayé d'imiter Friendster, mais on changeant un peu le concept en se concentrant sur un sujet précis comme l'origine démographique des utilisateurs, les intérêts en commun entre les utilisateurs (*Dogster*), les associations caritatives (*Care2*) ou même la religion (*MyChurch*) pour connecter les chrétiens avec leurs églises. D'autres ont choisi le réseau social professionnel en surfant sur le même domaine que *LinkedIn* tel que *Xing* par exemple.

On a remarqué aussi l'apparition de nouveaux phénomènes liés à ces réseaux :

- La régionalisation de certains réseaux sociaux comme le cas de *Google Orkut* qui est devenu le réseau social préféré des Brésiliens et des Indiens, *Friendster* en Asie et les îles du Pacifique, *Mixi* au Japon, *Hi5* en Amérique latine...
- L'effet de masse qui change radicalement le rapport de force entre réseaux sociaux, comme *Friendster* a vu ses utilisateurs le quitter vers *MySpace* beaucoup plus souple sur la question des droits d'auteurs.
- La question de la sécurité et la protection de la vie privée commence à se poser pour ce genre de sites, surtout après l'affaire de *MySpace* en 2005<sup>3</sup> quand le site a été impliqué dans une série d'interactions à caractère sexuel entre adultes et mineurs et qui a donné lieu à une action judiciaire.

### 2.2.3 La domination de quelques réseaux sociaux sur le marché

En 2004, l'apparition Facebook est considérée comme le plus populaire réseau social de tous les temps. Il était destiné à lier les étudiants de Harvard. Pour y adhérer, un étudiant devait fournir son courriel harvard.edu. Puis petit à petit, il a commencé à intégrer d'autres universités et collèges.

À partir de 2005, Facebook est élargi pour inclure les élèves de secondaire, les professionnels et finalement tout le monde. L'évolution la plus significative dans

---

<sup>3</sup> <http://www.liberation.fr/vous/01012318352-aux-etats-unis-la-peur-pedophile>

Facebook, est la possibilité pour des développeurs extérieurs de créer des applications que les utilisateurs peuvent intégrer dans leurs profils. Cette nouveauté a bien sûr soulevé une nouvelle fois le problème de la sécurité dans les réseaux sociaux et plusieurs faits ont alimenté cette peur dont la dernière vient de la commissaire à la protection de la vie privée du Canada qui a lancé une enquête en raison des nombreuses plaintes émises par les utilisateurs qui sont mécontents des changements apportés à leurs paramètres de confidentialité<sup>4</sup>.

On note aussi l'apparition dans cette même année de *Ning.com*. C'est une plateforme en ligne qui permet à n'importe quel utilisateur de créer son propre réseau social dans le domaine qu'il choisit. Il a été décrit comme une révolution dans le domaine des réseaux sociaux tout autant que Facebook ou MySpace. Mais il a eu un certain succès dans le domaine éducatif puisqu'il est devenu le site de référence pour la création des réseaux sociaux éducatifs.

2010 a vu l'arrivée d'un nouveau réseau social, Google+. Dès son lancement, il a beaucoup fait parler de lui par les spécialistes et le grand public et pour cause, il est conçu pour s'intégrer avec la plupart des produits Google déjà bien en avance par rapport à la concurrence. On trouve entre autres le service de messagerie Gmail, l'application de visualisation de photo Picasa, le lecteur de flux d'information Google Reader, le service de carte géographique et de plan *Google Map*.

À chacun ses nouveautés et l'une des nouveautés les plus marquantes dans Google + la possibilité de géolocaliser n'importe quel utilisateur, donc de le suivre dans ses déplacements.

## 2.3 L'utilisation des réseaux sociaux

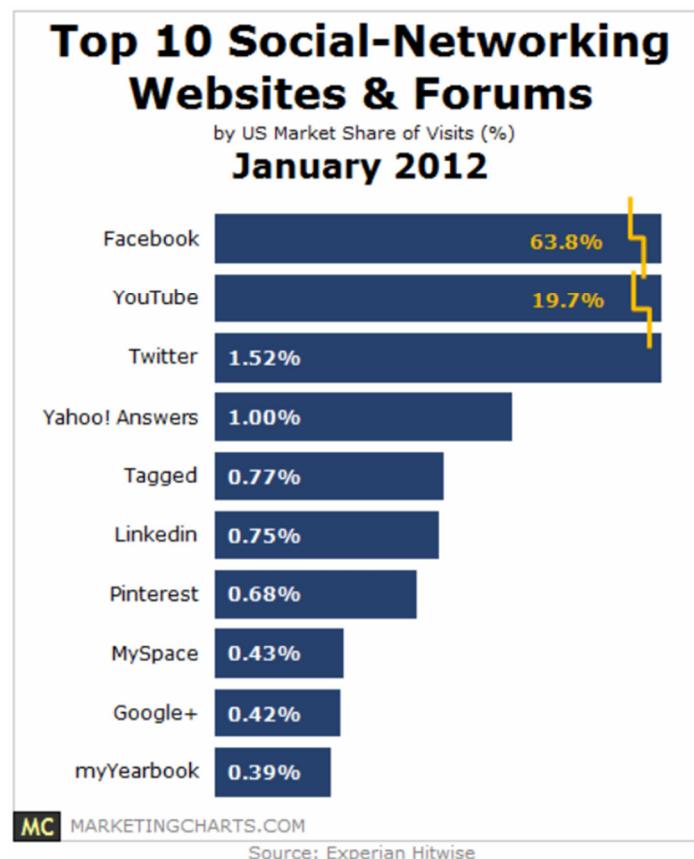
Experian Hitwise<sup>5</sup> a fait une étude en 2012 sur la part des 10 plus grands médias sociaux du trafic internet aux États-Unis. Cette étude a révélé que Facebook tient la plus grande part de marché avec 63,8% de nombre d'utilisateurs. Le réseau social qui vient

---

<sup>4</sup> [http://www.priv.gc.ca/cf-dc/2011/2011\\_005\\_0926\\_f.asp](http://www.priv.gc.ca/cf-dc/2011/2011_005_0926_f.asp)

<sup>5</sup> [http://weblogs.hitwise.com/james-murray/2012/04/instagram\\_snaps\\_into\\_top\\_10\\_so.html](http://weblogs.hitwise.com/james-murray/2012/04/instagram_snaps_into_top_10_so.html)

juste après avec un très grand écart est Twitter (1,52% du trafic). Ensuite on trouve le réseau social professionnel Linkedin avec 0,75%, MySpace avec 0,43% et enfin Google+ avec 0,42%. Ce graphe montre la dominance de Facebook sur tous les autres réseaux sociaux. Il montre également que malgré les moyens financiers et techniques investis par Google pour promouvoir Google+, il n'arrive pas à attirer les utilisateurs et reste très en retard par rapport à la concurrence. La figure 2 détaille tous ces résultats.

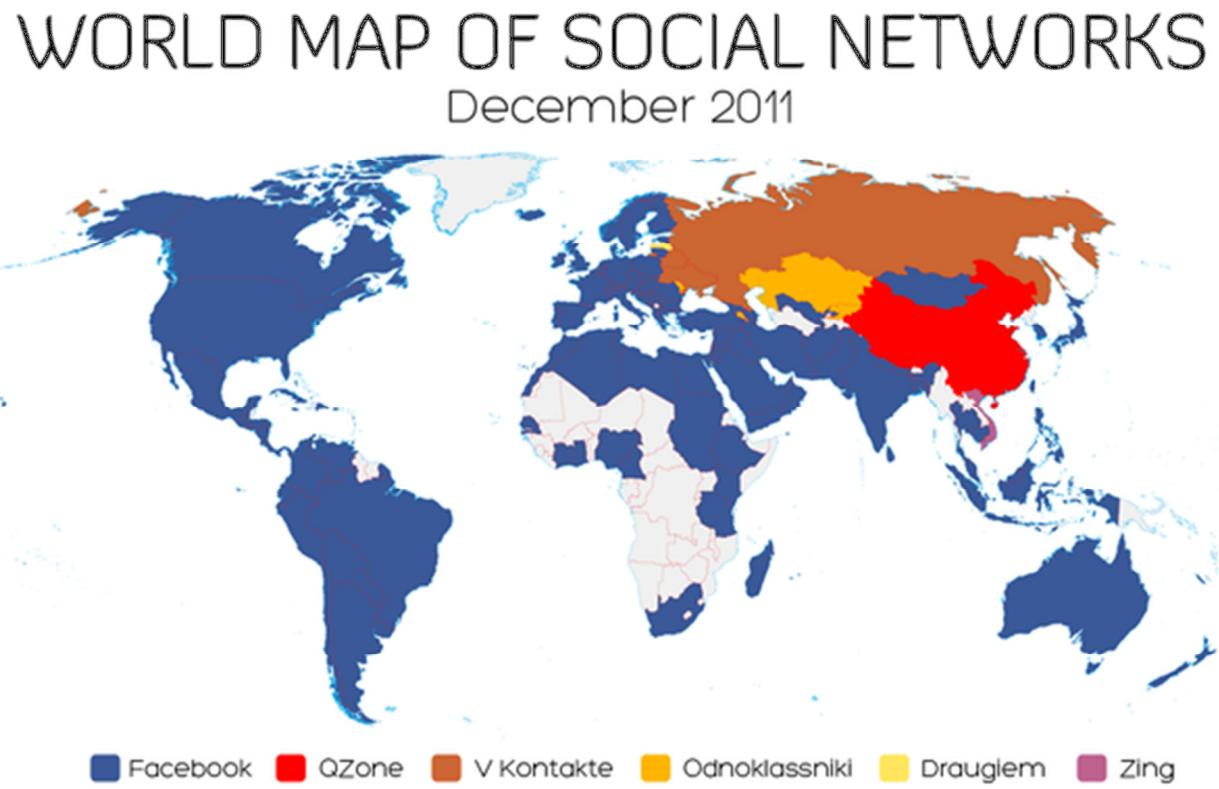


**Figure 2: Le top 10 des réseaux sociaux par taux de trafic**

En étudiant la carte mondiale des réseaux sociaux (figure 3) dans l'étude faite par Vincenzo Cosenza<sup>6</sup>, on peut remarquer la dominance de Facebook en Afrique, Europe, le continent américain et l'Asie du Sud. Le phénomène n'est pas pareil partout dans monde. Dans certains pays on trouve d'autres produits dominants. Comme QZone en Chine ou Vkontakte en Russie. Ceci peut être expliqué par la censure exercée par

<sup>6</sup> <http://vincos.it/world-map-of-social-networks/>

certains pays comme la Chine sur Facebook<sup>7</sup> ou encore la fierté nationale des Russes qui préfèrent leur produit local Vkontakte à Facebook<sup>8</sup>.



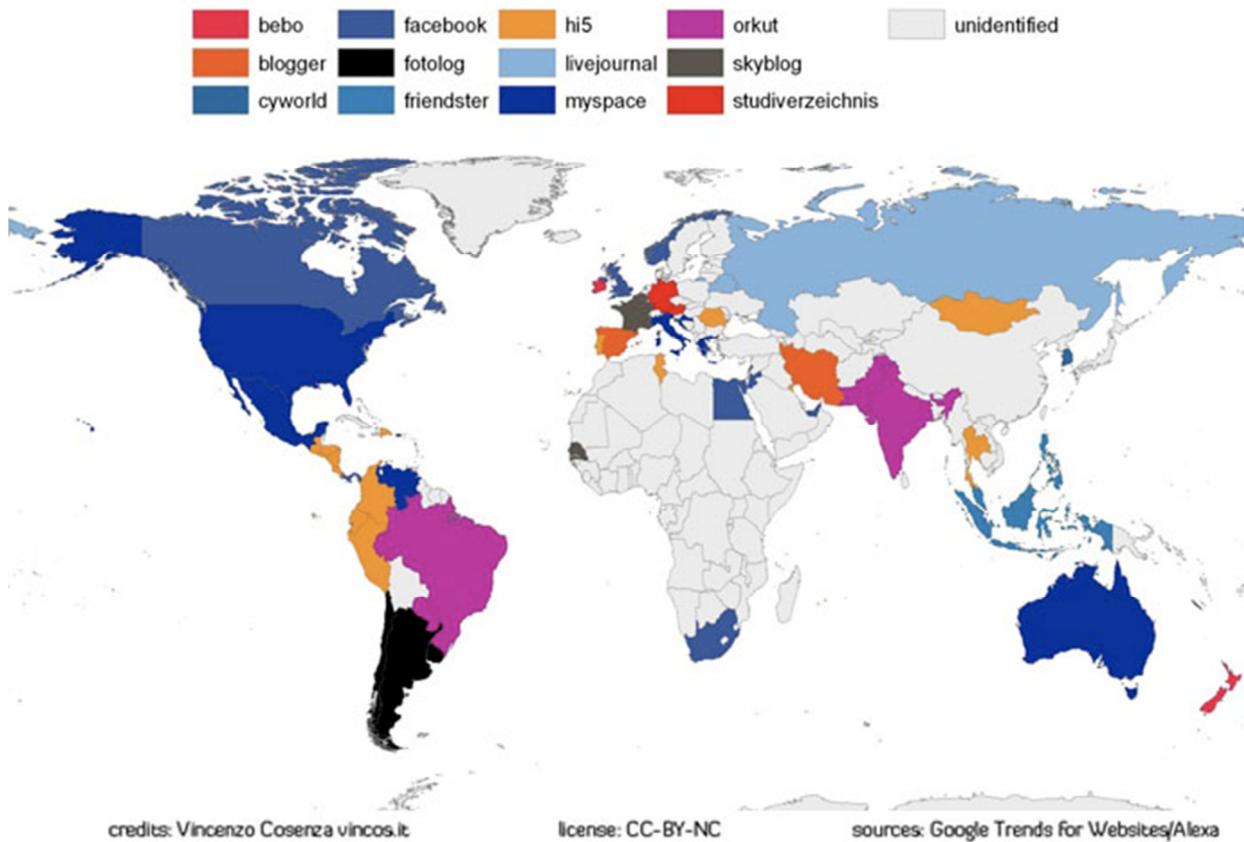
**Figure 3: Carte du monde des réseaux sociaux de 2011**

Si on compare cette étude à une autre étude faite en 2007<sup>9</sup>, on peut remarquer le changement rapide des habitudes des utilisateurs et le phénomène de mode des nouveaux réseaux sociaux. On voit bien en 2007 la large diversité de la concurrence et sa disparité par rapport aux pays. Facebook aux États-Unis, Mexique et en Australie, *Livejournal* en Russie, *cyworld* au Canada, *Orkut* au Brésil et en Inde. Ce qui n'est plus le cas en 2011.

<sup>7</sup> <http://www.rfi.fr/asie-pacifique/20120202-chine-reste-hors-portee-facebook-0>

<sup>8</sup> <http://vincos.it/2010/09/20/social-network-in-russia-facebook-vs-vkontakte/>

<sup>9</sup> <http://gawker.com/273201/the-world-map-of-social-networks>



**Figure 4: Carte du monde des réseaux sociaux de 2007**

### 2.3.1 Par rapport à l'âge des utilisateurs

Les sites de réseaux sociaux sont très populaires chez les jeunes entre 18 et 29 ans. Selon l'étude faite par PewInternet en 2011<sup>10</sup> représentée par la figure 5, l'année 2006 a vu exploser le nombre d'utilisateurs de cette tranche d'âge de 7% en 2005 à 49% en 2006. Ce boom était spécifique à cette tranche d'âge puisque durant cette même période, le nombre d'utilisateurs a diminué pour les 30 à 64 ans. Depuis cette date, le nombre d'utilisateurs de 18 à 29 ans a continué à grimper pour arriver à 86% en 2010 avec une légère diminution en 2011 (83%). On remarque le même phénomène pour les autres tranches d'âges, mais à moindre mesure. Le nombre d'utilisateurs entre 30 et 49 ans arrive à 70% du total, 51% pour les 50-64 ans et 33% pour les plus que 65 ans en 2011.

<sup>10</sup> <http://www.pewinternet.org/Reports/2011/Social-Networking-Sites/Report.aspx?view=all>

On peut donc conclure que les réseaux sociaux ont réussi à attirer toutes les tranches d'âges, même les plus vieux et que le nombre d'utilisateurs est en augmentation continue.

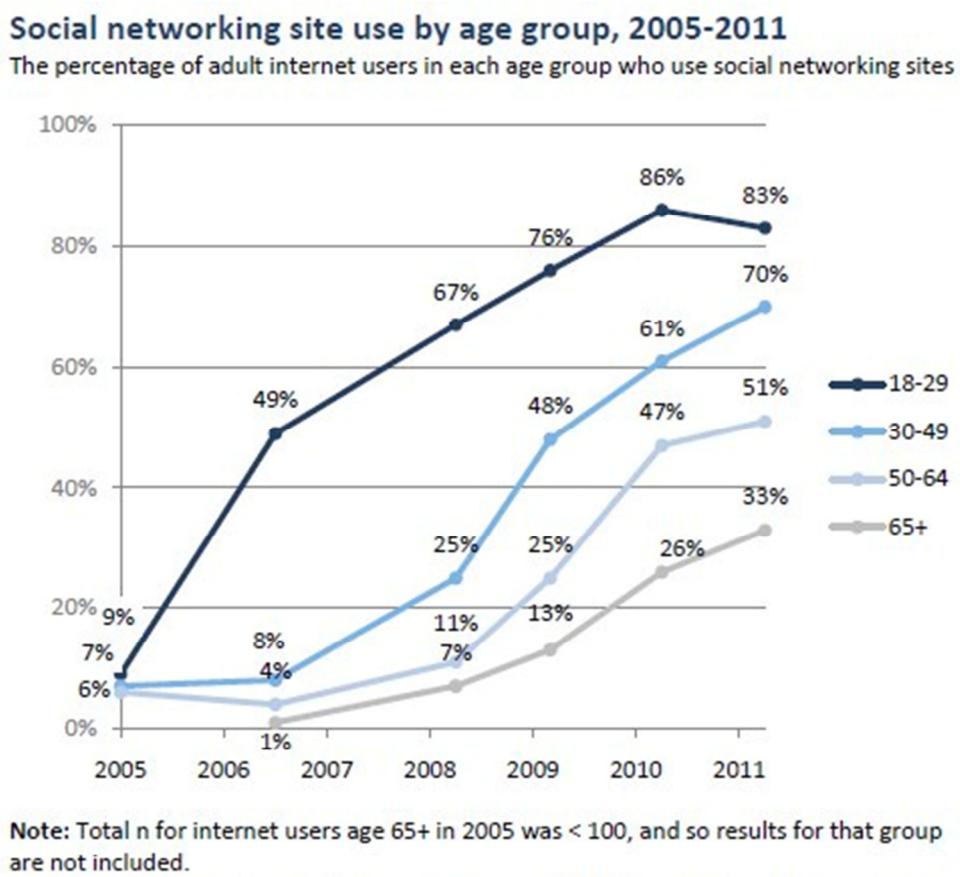


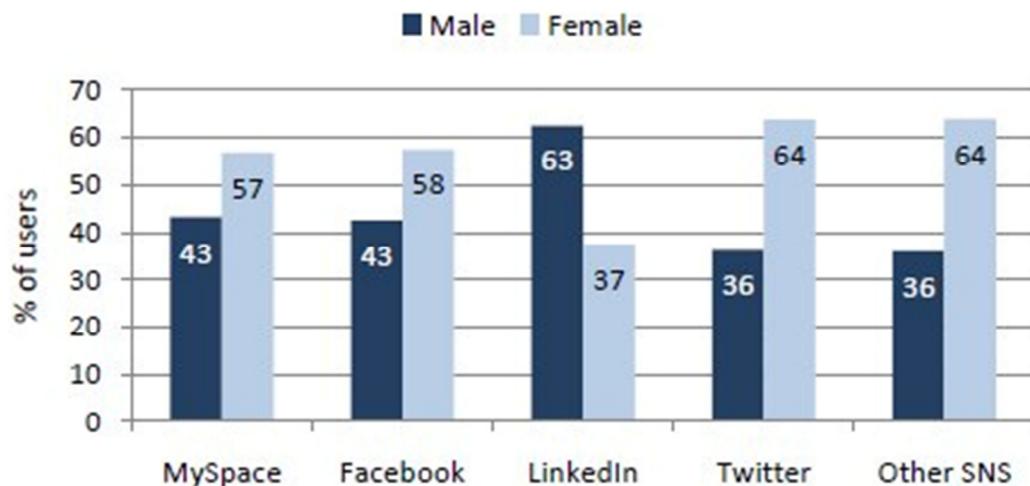
Figure 5: L'utilisation des réseaux sociaux par tranche d'âge entre 2005 et 2011

### 2.3.2 Par rapport au sexe des utilisateurs

Le même rapport fait par PewInternet en 2011 a étudié la distribution des utilisateurs selon le sexe dans différents réseaux sociaux (figure 6). On remarque clairement que les filles utilisent plus que les garçons les réseaux sociaux à l'exception de LinkedIn qui est plus accès professionnel. L'étude a révélé qu'on peut expliquer ce résultat par le fait que le nombre de filles dans le monde est largement plus grand que le nombre de garçons ce qui influence leurs nombres sur les réseaux sociaux aussi.

## Sex distribution by social networking site platform

*% of users on the following social networking sites who are male or female. For instance, 43% of MySpace users are male.*



**Source:** Pew Research Center's Internet & American Life Social Network Site survey conducted on landline and cell phone between October 20-November 28, 2010. N for full sample is 2,255 and margin of error is +/- 2.3 percentage points. N for social network site and Twitter users is 975 and margin of error is +/- 3.5 percentage points.

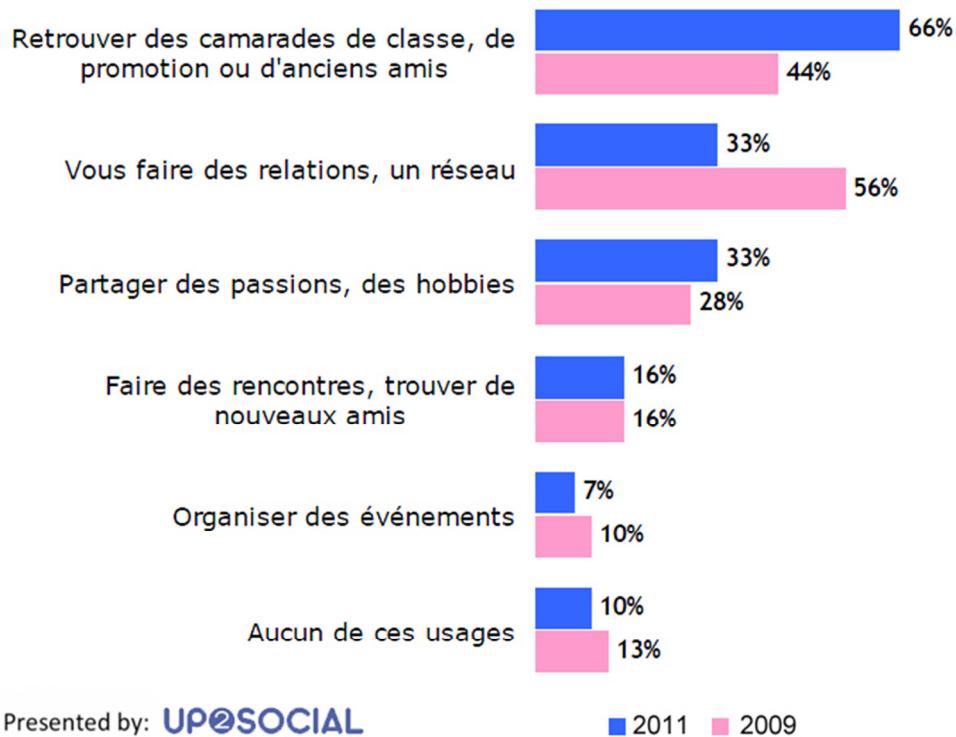
Figure 6: Comparaison entre les sexes dans les réseaux sociaux en 2010

## 2.4 Pourquoi utilise-t-on les réseaux sociaux

L'agence Up2Social (Up2social 2011) a détaillé les raisons de l'utilisation des réseaux sociaux. On peut extraire :

- Créer de nouvelles relations et augmenter la taille de son réseau.
- Retrouver des camarades de classe et d'anciens amis.
- Partager ces passions avec d'autres personnes qui ont les mêmes passions.
- Organiser des événements.
- Faire du réseautage pour un but professionnel (trouver un emploi).

La figure 7 explique mieux la disparité des utilisateurs suivant leur utilisation des réseaux sociaux.



**Figure 7: pour quelle raison les internautes utilisent les réseaux sociaux**

On remarque bien que la première raison pour laquelle on utilise ces sites consiste à trouver d'anciens camarades, ensuite faire de nouvelles relations et le partage des passions.

Ce classement n'était pas le même en 2009, où le but de faire de nouvelles rencontres était le plus prédominant. Ce changement d'habitude est dû aux caractères superficiels des relations virtuelles qui ont amené les utilisateurs à s'intéresser à renouer des relations avec des gens qu'ils connaissent étant donné que c'est plus durable et plus sérieux.

#### 2.4.1 Créer de nouvelles relations

On peut créer très facilement des relations avec quiconque inscrit dans les sites de réseaux sociaux. On cherche un profil suivant ses centres d'intérêt, son profil, son

travail ou bien simplement avec son nom. On lui envoie une demande d'ajout d'ami et s'il accepte, le demandeur peut voir d'autres détails de son profil. Il peut parler avec lui ou lui envoyer des messages.

Ce principe a été fortement influencé par les six degrés de séparations qui stipulent que chaque personne à six contacts qui le sépare de n'importe qui dans le monde. Ce degré de séparation est rendu plus court avec les sites de rencontre.

La figure 8 représente un aperçu d'un profil Facebook.

The screenshot shows Barack Obama's Facebook profile. At the top, there is a large portrait of him in a suit. Below the portrait, the URL 'WWW.WHITESHOWE.GOV' is visible, along with links to 'Become a Supporter', 'Add to my Page's Favorites', and 'View Updates'. A sidebar on the left contains the text: 'President Barack Obama is the 44th President of the United States of America.' Under the 'Information' section, it lists 'Current Office' as 'President of the United States'. The main content area shows a post from 'Barack Obama' titled 'Organizing for America | Tell Congress to Support President Obama's Budget'. The post includes a link to 'my.barackobama.com' and a description about supporting the president's budget. Another post below it is titled 'Open for Questions: President Obama Answers Your Questions' and includes a video thumbnail of Obama speaking. A third post at the bottom is titled '3/21/09: Your Weekly Address' and is a link to a YouTube video.

**Figure 8: Profil de Barack Obama sur Facebook**

## 2.4.2 Retrouver des camarades de classe et d'anciens amis

Plusieurs réseaux sociaux se sont spécialisés dans la rencontre entre les anciens camarades de classe, de travail ou d'anciens amis. On peut citer par exemple *Trombi.com*, *copainsdavant.com* ou encore *classmates.com* (figure 9).

Ce type de sites peut contenir tous les lieux où les utilisateurs ont partagé leur scolarité telle que les écoles, universités et lycées, ainsi que leurs activités associatives ou

professionnelles telles que les entreprises, les associations, les administrations et tous autres lieux où on peut rencontrer d'autres personnes et renouer des contacts avec eux.

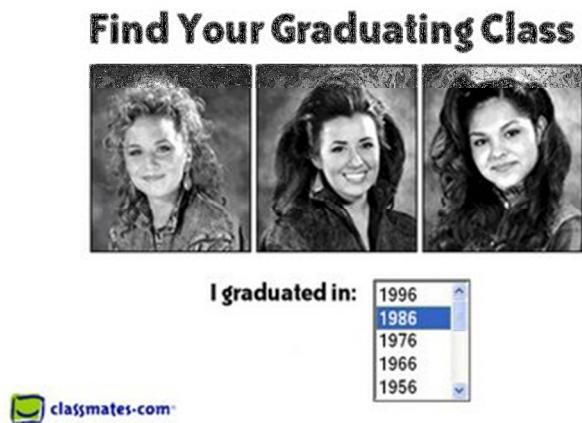


Figure 9: Recherche de classe suivant l'année de graduation sur Classmates.com

### 2.4.3 Partager ses passions

Dans tous les réseaux sociaux on trouve des groupes ou des personnes qui partagent les mêmes passions, passe-temps ou qui partagent les mêmes idées. Ces groupes permettent à leurs adhérents de partager les nouvelles actualités à ce sujet, les bonnes adresses et liens pour approfondir encore plus leur champ de connaissance, ils peuvent partager des images et vidéos liées à leur activité et organiser des rencontres pour se voir et pouvoir discuter (voir figure 10).

Figure 10: Groupe de Philatélie sur Facebook

#### 2.4.4 Organiser des événements

L'organisation des événements sur les réseaux sociaux est très utilisée par les internautes. Ces sites fournissent une publicité beaucoup plus large des événements que les simples affiches. Ainsi, les utilisateurs aident à les publier en les conseillant à leurs contacts. On trouve tous types d'activités : culturelles, politiques, artistiques, sportives (figure 11).

Figure 11: Évènement organisé sur LinkedIn

## 2.4.5 Trouver un emploi

Les réseaux sociaux jouent un rôle de plus en plus important pour les utilisateurs qui cherchent des emplois. Ces sites permettent de garder le contact avec des personnes qui peuvent aider le chercheur d'emploi tel qu'un ancien collègue ou un ancien camarade de classe. L'inscription sur ces sites permet aussi de se rendre visible pour les recruteurs et être toujours accessible pour les offres d'emplois mises en ligne par les contacts ou les agences spécialisées (figure 12).

**ilasalle Développement**  
Offre d'emploi : Chargé de projets 500-16HOM-PROJ chez [www.ilasalle.com](http://www.ilasalle.com)  
Montreal, Canadá y alrededores



**Poste actuel** • Offre d'emploi at ilasalle, filiale du Groupe Collège LaSalle

**Postes précédents** • Offre d'emploi - Experts de contenu (plusieurs mandats) 500-20HOM-EXP at ilasalle  
• Offre d'emploi - Infographiste (2 postes) 500-22HOM-INFO at ilasalle  
• Offre d'emploi - Chargé de projets 500-16HOM-PROJ at ilasalle

**Formation** • [www.ilasalle.com](http://www.ilasalle.com)

**→ Contacter ilasalle Développement**  
**→ Ajouter ilasalle Développement à votre réseau**

**Profil public généré par : LinkedIn**   
Créer un profil public : [S'identifier](#) ou [S'inscrire](#)

**Voir le profil complet de ilasalle Développement :**

- Voir qui vous et ilasalle Développement connaissez en commun
- Faites-vous présenter à ilasalle Développement

Figure 12: Offre d'emploi sur LinkedIn

# Chapitre 3 : Problématique

## 3.1 Risques encourus

Avec la montée en croissance des réseaux sociaux, de nouveaux utilisateurs vont se joindre à ces sites web, et en conséquence de nouveaux risques continueront à émerger dans le futur. Les risques les plus connus actuellement peuvent être résumés par ce qui suit (Aïmeur, Gambs et al. 2010; Timm and Perez 2010; Aïmeur and Schönfeld 2011; Ryan, Lavoie et al. 2011) :

**La notion trompeuse de communauté :** beaucoup de fournisseurs de réseaux sociaux disent qu'ils ont apporté les structures de communication du monde "réel" dans le "cyberespace". Ils affirment par exemple que la publication de données personnelles sur ces plateformes est sans risque. Cela est dû au partage d'informations entre amis comme on le fait en tête à tête. Si les utilisateurs ne sont pas informés sur la façon dont leurs informations de profils sont partagées ni sur la manière de les protéger, ils pourraient être séduits par cette notion de "communauté" et être encouragés à partager des renseignements personnels.

**Difficulté de fermer le compte d'un utilisateur :** les données, une fois publiées, peuvent rester stockées longtemps même lorsque l'utilisateur les aura supprimées du site original. Il peut exister des copies sur d'autres sites tiers ou même chez d'autres usagers. De plus, certains fournisseurs de service ignorent carrément toute demande de suppression de données ou de profils de leurs utilisateurs.

**Collecte de données secondaires par les fournisseurs de services :** Les fournisseurs de ces réseaux sociaux peuvent recueillir beaucoup d'informations secondaires sur leurs utilisateurs telles que leurs emplacements géographiques, leurs habitudes, leurs goûts ou leurs préférences afin de personnaliser leurs services pour le ciblage, la discrimination et le transfert des données aux tiers pour les revendre.

**Reconnaissance faciale :** les photos publiées peuvent devenir des identificateurs biométriques. Les logiciels de reconnaissance faciale ont été spectaculairement améliorés au cours des dernières années. Une fois qu'un nom est affecté à un visage dans une photo, il devient relativement facile de le retrouver dans d'autres photos. Cela met en danger sa vie privée et sa sécurité ainsi que celles de ses amis présents dans ces photos.

**Exploration et fouille des données (Datawarehouse and Datamining) :** Avec les traces que les utilisateurs des réseaux sociaux laissent derrière eux, il est possible de définir un profil sociodémographique et de cibler leurs modes de consommation. C'est une des méthodes utilisées par les réseaux sociaux pour faire du profit, car ils vendent ces informations à des sociétés commerciales. Elles leur permettent de faire des statistiques ou de la publicité dirigée en fonction des profils.

**Cyberintimidation :** les réseaux sociaux peuvent être utilisés pour intimider, harceler ou humilier certains utilisateurs. C'est certainement le plus gros risque chez les jeunes, car cela peut les amener à se sous-estimer, à devenir anxieux, dépressif et violent, et peut même les pousser au suicide.

Ainsi, on peut dire que très souvent le comportement de l'utilisateur des réseaux sociaux met en danger sa vie privée et celle de ses proches. Pour cela, il doit disposer des outils appropriés qui vont lui permettre de renforcer la protection de ses renseignements personnels.

La popularité des réseaux sociaux tels que Facebook, Twitter ou Google + fait d'elles des cibles attrayantes pour les pirates et les fraudeurs. Surtout que le principe de réseau qui permet l'accès à des comptes amis et la propagation très rapide de l'information, ainsi que les API ouvertes font de ce type de sites un moyen efficace pour les attaquants. Timm et Perez (Timm and Perez 2010) ont dénombré 3 attaques majeures très utilisées par les pirates sur les réseaux sociaux pour voler des informations personnelles et les utiliser dans des opérations frauduleuses. Ces attaques seront détaillées dans la partie suivante.

## 3.2 Techniques de fraudes utilisées

La fraude sur internet existe depuis les premiers jours d'internet. Chaque année, des internautes malveillants développent de nouvelles techniques destinées à tromper leurs victimes.

Ces mêmes techniques sont utilisées dans les réseaux sociaux, en utilisant les caractéristiques de ses plateformes qui sont le principe du réseau, la liste de contacts et les applications.

### 3.2.1 Le Spamming

Le spamming est l'envoi de messages non sollicités de façon automatique. Il s'agit en général d'envois en grande quantité d'annonces publicitaires. Mais elle ne se limite pas seulement aux annonces publicitaires, elles peuvent être aussi des courriels envoyés par des escrocs prétendant l'enrichissement rapide (travail à domicile, vente de produits miracles), l'attaque de virus, l'hameçonnage (récupération des données privées de la victime) (Stone-Gross, Holz et al. 2011).

Bien que la forme la plus connue des spams soit les courriels électroniques, elle peut s'étendre vers d'autres techniques comme les messageries électroniques, les groupes de discussions, les moteurs de recherches, les blogs, les messages téléphoniques et tout récemment les réseaux sociaux ... Le spamming est l'une des attaques les plus classiques qu'on retrouve sur internet. Elle est toujours en amélioration pour être plus efficace et pour qu'elle puisse détourner les techniques de protection. Elle s'adapte aussi aux nouvelles technologies comme les messageries instantanées, mais surtout aux réseaux sociaux où elle a trouvé un champ encore vierge et nouveau. Le spamming profite du principe du réseau qui lui permet de se transférer très rapidement surtout que des millions d'utilisateurs s'inscrivent chaque jour à ces sites. Les spameurs profitent de la popularité de ces sites pour concevoir de nouvelles techniques de spamming. Ces techniques utilisent les différents services offerts comme le service de messagerie qui permet aux utilisateurs d'envoyer des messages les uns aux autres. Ceci fournit un point de départ facile aux spameurs.

La plupart des réseaux sociaux comme Facebook et Google+ ne permettent à un utilisateur de commenter des publications d'un autre utilisateur que si ces deux utilisateurs sont amis. Pour contourner cette restriction, les spameurs créent des comptes fictifs et envoient aléatoirement des demandes d'amis. Une fois accepté, le spameur peut commencer à envoyer des messages de spam. Lorsqu'une victime clique sur le lien, un script est exécuté. Il permet de faire automatiquement les mêmes procédures pour tous les contacts de la victime. Cette technique, bien que compliquée, mais très répandue sur les réseaux sociaux comme Facebook, permet d'avoir le plus grand nombre de victimes, surtout que ces derniers deviennent un point de départ pour attaquer leurs amis. À ce stade, l'attaque devient plus efficace puisque si la première attaque était basée sur un compte fictif créé par le spameur, les victimes du spamming ajoutent de la crédibilité à l'attaque suivante à cause du lien de connaissance avec leurs amis. Et les victimes suivantes sont plus disposées à ouvrir les messages de quelqu'un qu'ils connaissent. D'autres variantes d'attaques incluent le spam dans les commentaires des photos d'autres personnes, dans les invitations à des événements ou des messages postés directement sur le mur de la victime<sup>11</sup>. Ces nouvelles variantes permettent d'attaquer non pas la victime, mais aussi tous ceux qui accèdent au lien attaqué. Donc, avoir un public plus large.

Dans tous les lieux où les gens peuvent saisir des informations, les spameurs placent des publicités, que ce soit des messages directs, des mises à jour de statuts, des commentaires sur des vidéos ou bien des demandes de contacts. Des techniques de spam permettent même de générer des messages sur différentes plateformes en simultané. Un spam peut s'envoyer vers le compte Facebook de la victime et en simultané vers son courriel.

Kaspersky Lab a fait une étude sur le Spaming en 2012<sup>12</sup> (figure 13). Elle a déterminé que l'Inde est le pays à partir duquel on envoie le plus de spams dans le monde. Il représente 16,35% du volume total de spam. Ce pourcentage a augmenté de 5% par rapport à 2010. La Russie vient septième du classement avec un pourcentage de 3.2%.

---

<sup>11</sup> <http://comarround.wordpress.com/2011/10/05/spam-trends-for-2011/>

<sup>12</sup> [http://www.securelist.com/en/blog/545/New\\_spam\\_sources\\_in\\_the\\_making](http://www.securelist.com/en/blog/545/New_spam_sources_in_the_making)

Ce pourcentage a diminué de 0.7% par rapport à 2010. Le Brésil a subi la croissance la plus grande, occupant la 2e place avec 11,22% du volume total de spam, en augmentation de 4,36% par rapport à 2010. Et enfin la Corée du Sud a subi la diminution la plus grande du classement qui a chuté de 2,63% la faisant passer à la 4e position avec 5,6% du total.

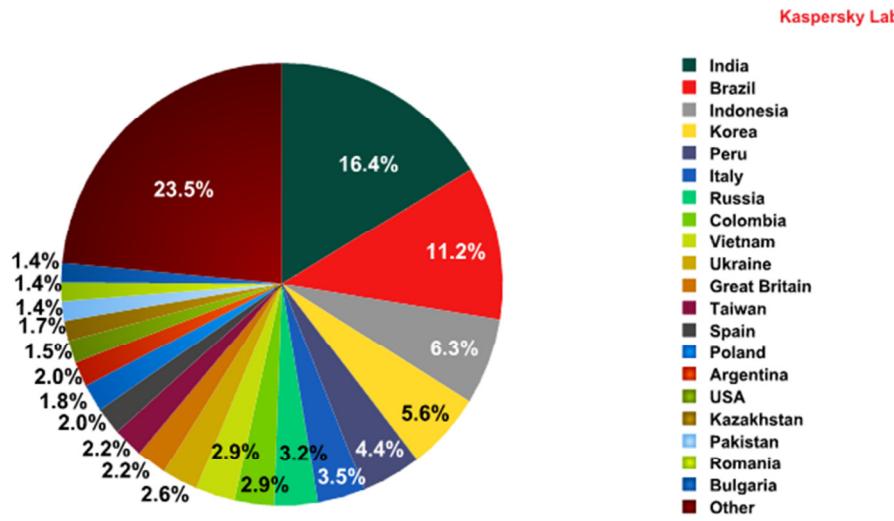


Figure 13: Sources des spams en juin 2012

Une autre étude faite dans le même rapport (figure 14) montre que le tiers de tous les spams envoyés est considéré comme fraudes informatiques. Ce taux montre clairement le danger que subissent les internautes s'ils sont mal informés. Surtout que ces spams attaquent en premier lieu les boîtes électroniques sous la forme de messages qui peuvent contenir des pièces jointes malveillantes ou des liens vers des sites malveillants.

Comme exemple, plus d'un quart des spams contiennent des publicités pharmaceutiques. On observe ces derniers temps le grand phénomène des publicités qui vantent le bienfait de certains médicaments comme le Viagra ou les ajouts nutritifs pour sportifs. En totale infraction des avertissements des professionnels de la santé et des gouvernements. Et même si l'utilisateur ne compte pas acheter ces médicaments, mais rien que le fait de visiter les sites propriétaires de ces annonces peuvent mettre l'utilisateur à des risques d'attaque informatique.

Autres types de spam très répandu et qu'on trouve dans le graphique on note aussi les spams financiers qui prédisent un gain très rapide d'argent ou des prêts douteux. Ce type de spam représente 12,1% du total des spams envoyé.

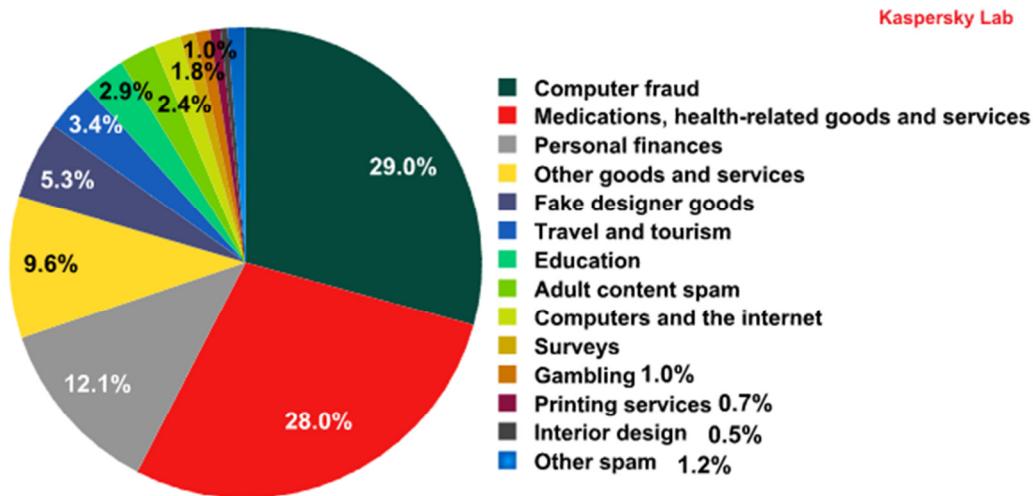


Figure 14: Spams par catégories

Plusieurs solutions ont été mises en place pour contrer ces attaques, on peut citer les tests CAPTCHA pour éviter l'envoi automatique de messages. Les CAPTCHAS sont des tests ayant pour but de s'assurer que le traitement en cours est fait par un humain, et non pas généré par un ordinateur. Ils sont surtout utilisés sur internet dans les formulaires pour éviter les soumissions automatisées et de grandes masses réalisées par des robots. La vérification se fait à travers l'analyse d'une image ou d'un son par un humain.

Cette technique ralentit le spam, mais malheureusement ne l'arrête pas. La plupart des techniques de CAPTCHA ont été brisées, mais les chercheurs essayent toujours de les améliorer pour arriver à des méthodes plus sûres<sup>13</sup>.

Une autre méthode mise en place c'est la détection des comptes frauduleux, ceci pour prévenir contre l'utilisation de plusieurs comptes par les pirates pour lancer leurs attaques de spam. En effet, les sites de réseaux sociaux mettent des systèmes qui comptent le nombre de messages envoyés et bloquent le compte qui dépasse une

<sup>13</sup> <http://www.xmco.fr/article-captcha.html>

certaine limite dépendamment de l'utilisation du compte (fréquence d'utilisation, durée de connexion, taux d'envoi de courriels...)<sup>14</sup>. Ils offrent aussi une fonctionnalité permettant de signaler les messages définis par les utilisateurs comme étant des spams, ce qui leur permet de les bloquer à l'avenir même si envoyés à travers d'autres comptes.

### 3.2.2 Le phishing (Hameçonnage)

Le phishing se définit comme un ensemble de techniques utilisées par les pirates pour collecter des renseignements personnels d'internautes peu méfiants. Il se présente par l'utilisation des pirates de sites web et courriels qui imitent ceux d'institutions financières, d'organismes gouvernementaux ou bien de grandes marques connues et dignes de confiance. Ces pirates arrivent souvent à convaincre les internautes à divulguer des informations privées liées à leurs banques telles que le nom d'utilisateur, le mot de passe, le numéro de carte de crédit ou l'adresse (Coronges, Dodge et al. 2012).

Le phishing connaît une croissance rapide suivie d'une augmentation du nombre d'escroqueries et de vols d'identité sur internet. Une étude faite par the Canadian Anti-Fraud Centre en 2011<sup>15</sup> a déterminé que les criminels sont en mesure de convaincre jusqu'à 5% des personnes visées de répondre à leurs courriels. Le problème avec le phishing c'est qu'il est en constante évolution. Les pirates trouvent toujours de nouvelles méthodes pour contourner les contrôles informatiques et ainsi avoir toujours plus de victimes. Les méthodes les plus utilisées dans le fishing selon Hong (Hong 2012) sont :

**Le spear phishing :** C'est une forme de phishing qui vise une organisation spécifique pour chercher un accès non autorisé à des données confidentielles<sup>16</sup>. Souvent le but de ces attaques est lucratif, il peut porter sur le secret commercial ou bien sur le renseignement militaire. Pour arriver à leur fin, les pirates envoient des courriels

---

<sup>14</sup> <http://partenaire-webmarketing.com/blog/facebook-des-amis-oui-mais-pas-trop-vite>

<sup>15</sup> [http://www.antifraudcentre-centreantifraude.ca/english/documents/QuarterlyStatisticalReport\\_Jul-Sep2011.pdf](http://www.antifraudcentre-centreantifraude.ca/english/documents/QuarterlyStatisticalReport_Jul-Sep2011.pdf)

<sup>16</sup> <http://searchsecurity.techtarget.com/definition/spear-phishing>

apparaissant comme s'ils viennent d'une grande entreprise ou bien d'un site web très convoité comme eBay ou bien PayPal.

**Le phishing vocal** : Il ressemble au phishing classique, mais au lieu de fournir un lien frauduleux pour que le client clique dessus, il donne un numéro de téléphone. Ce type d'arnaque utilise le plus souvent des fonctionnalités de téléphonie IP difficilement contrôlable par les gouvernements et à faible cout pour exploiter la confiance de l'utilisateur dans les services de téléphones fixes. Ce qui facilite l'accès aux informations personnelles et financière des internautes.

Dans le cas des réseaux sociaux, la plupart d'entre elles contiennent des services de messagerie électronique qui peuvent être utilisés pour des attaques de phishing. Mais la nouveauté réside dans le fait que les pirates peuvent utiliser les caractéristiques des réseaux sociaux pour identifier le cercle d'amis des victimes et récolter de grandes quantités d'informations affichées publiquement sur leurs comptes. Des informations comme l'emploi actuel ou l'institution fréquentée peuvent constituer une base de départ pour des campagnes de phishing bien ciblées destinées à des employés d'une même entreprise ou des étudiants d'une même institution. Ils peuvent aussi utiliser des informations personnelles affichées sur le compte comme le nom et prénom ou bien l'adresse pour envoyer des courriels qui contiennent des informations réelles et ainsi devenir plus crédibles aux vues des victimes.

Dans le rapport bimestriel de la APWG (Anti-Phishing Working Group)<sup>17</sup>, plusieurs statistiques sont faites pour étudier le phénomène du phishing à travers le monde. En 2011, plus de 112,472 attaques de type phishing ont été signalées à travers le monde. C'est beaucoup plus que les 42,624 attaques observées en 2010, mais moins que le record observé en 2009 qui était de 126,697 attaques et qui était dû au boom des attaques de type Botnet (machines zombies)<sup>18</sup> maîtrisé par la plupart des antivirus actuels. Ils ont précisé que l'augmentation du nombre d'attaques par rapport à 2010 est due à l'augmentation rapide du nombre de victimes d'origine chinoise. Ceci vient en

---

<sup>17</sup> [http://www.antiphishing.org/reports/apwg\\_trends\\_report\\_h1\\_2011.pdf](http://www.antiphishing.org/reports/apwg_trends_report_h1_2011.pdf)

<sup>18</sup> <http://www.microsoft.com/security/pc-security/botnet.aspx>

parallèle avec la situation économique nouvelle que vie actuellement la chine et qui se caractérise par l'ouverture de l'économie chinoise au commerce électronique.

Plusieurs autres observations ont été faites dans le rapport :

- Les pirates ont utilisé pour leurs attaques 79,753 noms de domaines. Ce nombre est le plus fort observé par l'organisation. Il est dû aussi au boom de l'augmentation des nombres d'attaques à destination de la Chine.
- Parmi ces noms de domaines utilisés pour le phishing, 2,385 attaques ont été faites à partir d'adresses IP uniques.
- Parmi les 79,753 domaines utilisés pour le phishing, l'organisation a identifié 14,650 domaines enregistrés directement par les pirates (18% du total). Alors qu'il était de l'ordre de 28% en 2010. Le reste des domaines (82% du total) ont été piratés et détournés d'hébergeurs web vulnérables.
- L'organisation a trouvé 520 établissements ciblés par les campagnes de phishing. Il s'agit de banques, sites d'e-commerce, sites de réseaux sociaux, fournisseurs d'accès internet, services fiscaux gouvernementaux, services postaux...

Le tableau suivant présente les résultats en détail :

**Tableau 1: Statistiques sur le phishing fait par APWG**

Type d'attaque	1H2011	2H2010	1H2010	2H2009	1H2009
Noms de domaines utilisés pour le phishing	79,753	42,624	28,646	28,775	30,131
Nombre d'attaques	115,472	67,677	48,244	126,697	55,698
Nombre d'attaques à travers des adresses IP uniques.	2,385	2,318	2,018	2,031	3,563
Domaines enregistrés pour le phishing	14,650	11,769	4,755	6,372	4,382

Une autre étude faite par Kaspersky Lab en juin 2011<sup>19</sup> a déterminé que la quantité de courriels de phishing représente 0,02% du nombre total de courriels envoyés.

Elle a présenté aussi les 10 organisations les plus ciblées par les campagnes de phishing. La figure suivante décrit ce classement.

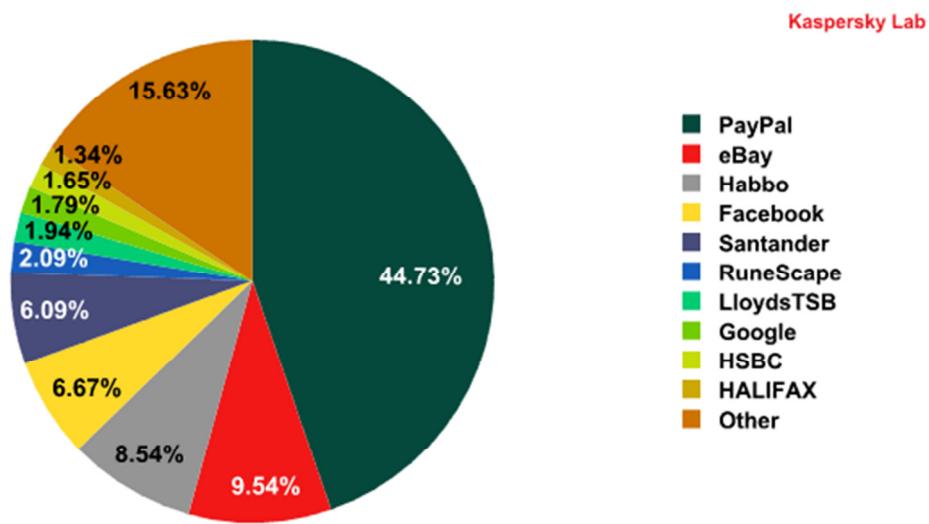


Figure 15: Le top 10 des organisations visées par les attaques de phishing en juin 2011

La majeure partie des campagnes de phishing (44,73% du total) est destinée au service de paiement en ligne PayPal. Ceci est dû à sa notoriété : c'est le site de paiement en ligne le plus utilisé au monde, donc plus susceptible de subir des attaques de phishing.

Facebook, le réseau social le plus utilisé au monde est classé comme la 4e compagnie la plus attaquée par des campagnes de phishing avec 6,67% des attaques. Un autre réseau social dans le classement est Habbo, destiné aux jeunes. Il est classé 3e avec 8,54%.

### 3.2.3 Le vol d'identité

Le vol d'identité est le fait de voler l'identité d'une personne et se faire passer pour cette même personne dans le but d'accéder à ses ressources ou faire des transactions en son nom. Cela peut être pour différents buts : avoir un crédit, acheter des marchandises en

<sup>19</sup> [http://www.securelist.com/en/analysis/204792183/Spam\\_report\\_June\\_2011](http://www.securelist.com/en/analysis/204792183/Spam_report_June_2011)

son nom ou profiter de services réservés à la victime en utilisant ses documents personnels comme son passeport ou son assurance de santé. Il y a souvent des conséquences négatives pour les victimes du vol d'identité puisqu'elles seront tenues responsables des effractions de l'agresseur. Les organismes ciblés par les arnaqueurs peuvent avoir aussi des répercussions négatives puisqu'ils vont subir des pertes économiques.

Le vol d'identité se réalise lorsqu'une entité collecte et utilise des renseignements personnels d'une personne physique ou morale d'une façon non autorisée dans l'intention de frauder ou commettre n'importe quel autre crime<sup>20</sup>.

Power (Power 2011) a catégorisé le vol d'identité en deux groupes :

### ***3.2.3.1 Vol d'identité classique***

**Fouille de poubelles** : le fraudeur fouille dans les poubelles et essaye de trouver le maximum de feuilles contenant des données privées. C'est le moyen le plus courant que font les fraudeurs pour obtenir des informations qui peuvent contenir les chèques, cartes de crédit, relevés bancaires et n'importe quels autres documents qui contiennent des renseignements personnels.

**Espionnage** : c'est le fait de regarder par-dessus l'épaule de quelqu'un lorsqu'il est en train de payer avec sa carte bancaire dans un commerce ou dans un guichet automatique. L'espion peut récupérer le numéro de la carte bancaire et le mot de passe qui permettent de l'utiliser.

**Appels téléphoniques mensongers** : le fraudeur communique avec la banque ou la compagnie de téléphone de la victime en faisant semblant d'être ce client et demande des informations de son compte. Cette fraude peut se faire aussi en accédant au compte en ligne de cette victime (services bancaires en ligne).

**Vol d'objets personnels** : lorsque quelqu'un vol un objet personnel contenant des données sensibles comme le vol d'ordinateurs ou des portefeuilles. Ceci touche aussi

---

<sup>20</sup> <http://www.cippic.ca/sites/default/files/LawEnforcement.pdf>

bien des particuliers que des entreprises. La fraude peut se faire en achetant les informations de l'entreprise à un employé malhonnête.

**Scan des cartes bancaires :** Le fraudeur installe un mécanisme lui permettant de scanner les cartes bancaires ou de crédits à partir des lecteurs de cartes dans les commerces ou les distributeurs électroniques des banques sans que la victime ne se rende compte. Ces données sont transmises vers d'autres cartes frauduleuses.

La forme la plus commune du vol d'identité se fait à travers l'accès aux informations collectées dans les lieux publics (services postaux), le vol d'objets personnels (sac à main), prise de contrôle de bases de données (vol des numéros de carte de crédit).

### **3.2.3.2 Vol d'identité en ligne**

Il y a plusieurs façons d'obtenir en ligne les informations personnelles des victimes :

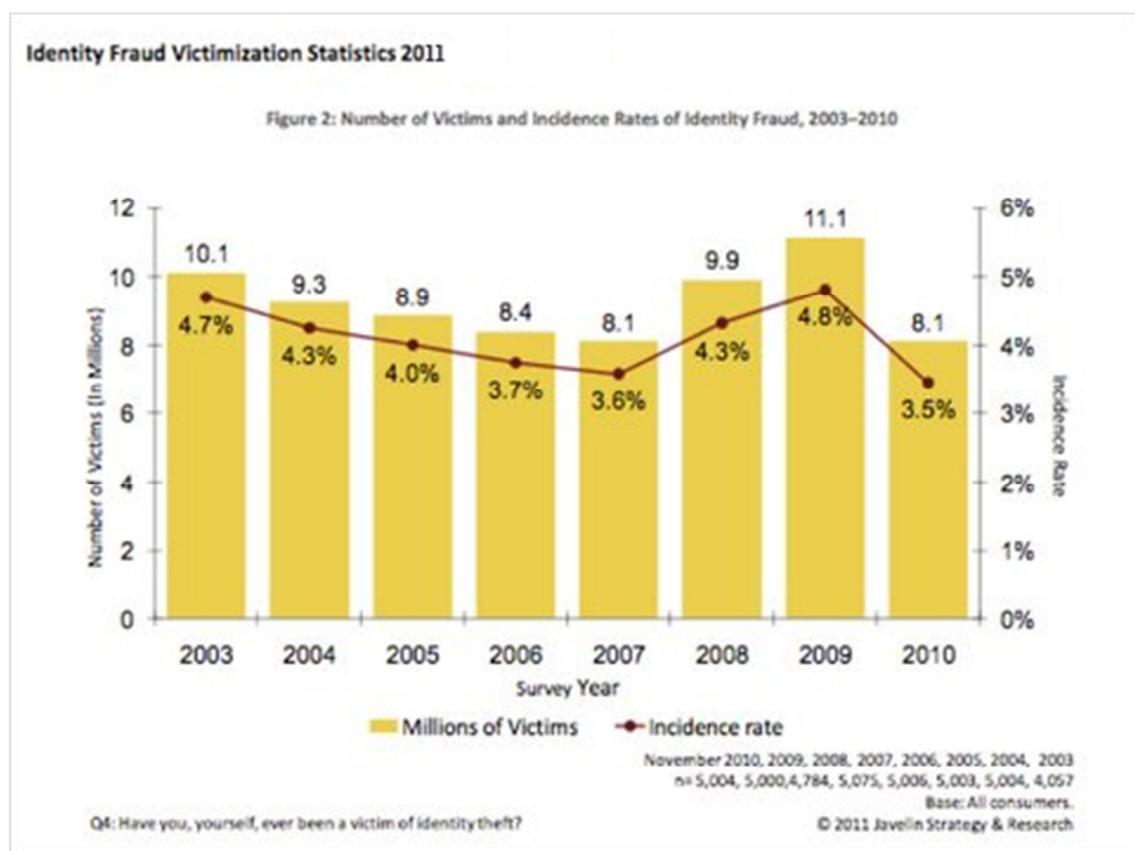
**Les malwares :** Ce sont des logiciels malveillants installés à l'insu de la victime, conçus pour collecter des informations sensibles et pour obtenir un accès non autorisé aux systèmes informatiques. Il existe plusieurs types de malwares, dont les plus dangereux sont les Keylogging. Ce sont des logiciels malveillants qui interceptent les frappes de claviers faites par la victime sans qu'elle ne se rende compte. Ils peuvent intercepter les mots de passe, messages privés et n'importe quelles informations saisies par l'utilisateur. Toutes ces informations sont ensuite envoyées aux fraudeurs qui les analysent et trient les données sensibles.

**Spamming :** Ce sont des communications électroniques non sollicitées envoyées vers les boîtes courriels. Il s'agit normalement d'envoi de grandes quantités de courriels publicitaires. Cette attaque est décrite en détail à la section 3.a.

**Phishing :** Ce sont des techniques utilisées par les fraudeurs afin d'obtenir des informations confidentielles des victimes. Elles consistent à prendre l'apparence de sites web d'institutions comme les banques, administrations ou compagnies de téléphones. Les victimes pensant qu'ils s'adressent à leurs institutions saisissent des informations

confidentielles comme les mots de passe, numéros de carte de crédit et adresses de résidences. Cette attaque est décrite en détail à la section 3.b.

Selon le rapport de 2011 sur les fraudes liées au vol d'identité fait par Javelin Strategy and research<sup>21</sup> (figure 16), le nombre estimé de victimes de vol d'identité a fortement baissé en 2010 par rapport à 2009. Il est passé à 8.1 millions d'adultes aux États-Unis en baisse de 28%. Ceci représente la diminution la plus forte depuis 2003 observée par Javelin.



**Figure 16: Le nombre de victimes de vol d'identité**

James Van Dyke, le président et fondateur de Javelin Strategy & Recherche, a expliqué la diminution du nombre des victimes de vol d'identité et le montant total de la fraude annuelle pour le fait que les entreprises ont fait de très grands efforts pour réduire ce

<sup>21</sup> [http://bucks.blogs.nytimes.com/2011/02/09/the-rising-cost-of-identity-theft-for-consumers/#p\[AtsSci\]](http://bucks.blogs.nytimes.com/2011/02/09/the-rising-cost-of-identity-theft-for-consumers/#p[AtsSci])

type de fraude. L'industrie bancaire et les gouvernements ont pris beaucoup de mesures pour éduquer et prévenir les consommateurs et résoudre de telles fraudes. Les consommateurs font le suivi de leur compte plus régulièrement et avec plus de soin. Côté gouvernement, plus les mesures de sécurité sont prises et plus les forces de l'ordre prennent ce problème avec sérieux.

Pour l'augmentation des sommes perdus, James Van Dyke a expliqué ça par les moyens de fraudes de plus en plus sophistiqués. Il a noté par exemple :

Le vol à partir d'un nouveau compte créé à l'insu de son propriétaire non pas à partir d'un compte bancaire existant. La victime peut rester un certain temps sans se rendre compte de ce nouveau compte à partir duquel le fraudeur peut faire n'importe quelle opération.

L'augmentation des fraudes amicales durant lesquels une connaissance de la personne fait ce vol. Ces amis peuvent non pas seulement voler de l'argent à leurs amis, mais aussi faire d'autres types d'opérations comme un abonnement téléphonique ou un abonnement à un câble.

Le vol par carte de débit qui est devenu plus fréquent que celui de vol par carte de crédit. Les clients habituer à entendre des alertes pour sécuriser leurs cartes de crédit ne prennent pas le temps de sécuriser leurs cartes de débit. Une autre raison tient au fait que les opérations de cartes de crédit sont plus faciles à détecter par les propriétaires. De plus, certaines sommes sont remboursables par les compagnies de crédits. Ce qui est n'est pas le cas des cartes de débit, ce qui expose la victime à des pertes plus grandes.

Durant tout ce chapitre, nous avons détaillé les risques que peut prendre un utilisateur malveillant s'il affiche ses données privées sur son compte. Nous avons aussi décrit des méthodes qu'utilisent les escrocs pour voler ces données privées et qu'est ce qu'ils sont capables de faire avec. Dans le chapitre suivant, nous allons décrire les études qui ont essayé de remédier à ce problème. Ensuite nous allons présenter notre méthodologie.

## Chapitre 4 : Les systèmes de protections de la vie privée

La forte expansion des réseaux sociaux et l'échange de grandes quantités de renseignements personnels et privés ont été extraordinaires sur Internet. Divers chercheurs ont montré que les réseaux sociaux peuvent constituer une menace importante pour les utilisateurs (Brown, Howe et al. 2008; Chew, Balfanz et al. 2008; Bilge, Strufe et al. 2009; Bonneau, Bonneau et al. 2009; Fogel and Nehmad 2009). Cette popularité croissante a conduit à de nombreuses études relatives à la sécurité et aux aspects de protection de la vie privée sur les réseaux sociaux (Aïmeur, Brassard et al. 2008; Yan and Ahmad 2008; Aïmeur, Gambs et al. 2010). Différents groupes de recherche ont essayé de comprendre les risques d'atteinte à la vie privée en se concentrant sur l'étude des types de fuites de données dues à des attaques ou à des profils accessibles publiquement (Bin and Jian 2008; Korolova, Motwani et al. 2008).

Nous allons faire dans la première partie un survol de quelques études qui ont touché la vie privée dans les réseaux sociaux. Ensuite nous nous concentrerons sur ceux qui se rapprochent le plus à la méthodologie que nous avons suivie pour Protect-U.

### 4.1 Survol

L'idée de collecter des données provenant de différentes sources pour créer un profil utilisateur a été étudiée dans différents contextes. Griffith et al. (Griffith and Jakobsson 2005) ont montré qu'il est possible de corrélérer les informations de profils publiques pour trouver le nom de jeune fille d'une femme mariée. D'autres recherches (Zheleva and Getoor 2009) ont montré que les informations non privées sur le profil d'un utilisateur peuvent également être déduites à l'aide d'informations contextuelles (par exemple, l'appartenance politique d'un utilisateur peut être prédite en examinant l'affiliation politique de ses amis). Certaines études ont montré qu'il est possible de reconstruire l'identité en corrélant les profils d'une personne sur plusieurs réseaux sociaux. Par

exemple, la corrélation est faite dans (Irani, Webb et al. 2009) en utilisant le pseudonyme ou le nom réel de l'utilisateur. Balduzzi et al. (Balduzzi, Platzer et al. 2010) ont étudié le fait de créer des comptes appartenant au même utilisateur avec la même adresse électronique sur plusieurs réseaux sociaux. Ils montrent que l'attaquant peut corrélérer les informations croisées entre les différents sites de réseaux sociaux de manière automatisée et ainsi détecter différents profils créés par cette personne.

Wondracek et al. (Narayanan and Shmatikov 2009) ont introduit une nouvelle technique basée sur le vol des informations à partir des pages de groupes. Ils ont montré que les groupes de Facebook peuvent révéler beaucoup d'informations sur la personne qui est abonnée. Une application tierce peut facilement récupérer ces groupes et associer les informations générées à la personne qui a exécuté cette application. Ils ont appliqué cette technique sur le réseau Xing et ils ont estimé qu'environ 42% des utilisateurs qui sont inscrits dans des groupes peuvent être identifiés de façon unique.

Afin d'améliorer la protection de la vie privée des utilisateurs des réseaux sociaux et leur compréhension des risques sur leur confidentialité, de nombreuses études utilisent l'approche « *Privacy Feedback and Awareness* » (PFA) (Lederer, Hong et al. 2004). Cette approche utilise les systèmes de recommandations dans le but d'assister les utilisateurs à maintenir un niveau élevé de compréhension de ces paramètres de confidentialité. Les utilisateurs divulguent des informations sensibles sur les sites de réseaux sociaux, parce qu'ils ne sont pas conscients des dangers de ces divulgations sur leurs vies privées. Dans le cas de la photo de profil d'un utilisateur par exemple, ses "paramètres de confidentialité" par défaut permettent à n'importe quel autre internaute de la voir. C'est pour cette raison que c'est très important de rendre les utilisateurs de réseaux sociaux conscients de cette réalité et leur permettre de prendre des décisions plus claires au sujet de leurs publications. Les systèmes de recommandation semblent être un bon moyen pour que les gens deviennent plus conscients, en leur donnant des commentaires et des conseils ciblés.

Fang, L. et K. LeFevre (Fang and LeFevre 2010) présentent l'Assistant de confidentialité « *Privacy Wizard* ». L'objectif de l'assistant est de configurer

automatiquement les paramètres de confidentialité de l'utilisateur. Pour ça, l'utilisateur fixe un ensemble de paramètres de confidentialité manuellement, et l'assistant utilise l'apprentissage machine (un classificateur) pour qu'il configure automatiquement le reste.

Mazzia, A.L.K. et E. Adar (Mazzia and Adar 2011) introduisent PViz, un système correspondant directement à la façon avec laquelle les modèles de groupes utilisateurs ainsi que les politiques de confidentialité sont appliqués à leurs réseaux. Il permet à l'utilisateur de comprendre la visibilité de son profil en fonction de la nature de ses groupes d'amis avec un niveau différent de granularité. PViz est centrée sur une interface graphique, qui montre le réseau social de l'utilisateur. Chaque nœud de l'affichage représente une sémantique significative d'un groupe d'amis de l'utilisateur ou un ami individuel.

Patil et A. Kobsa (Patil and Kobsa 2010) proposent PRISM un système qui fournit aux utilisateurs une messagerie Internet avec différentes visualisations. Il fournit des mécanismes pour se présenter de façon différente entre plusieurs groupes de contacts en sélectionnant un ensemble de paramètres pertinents spécifique à chaque groupe.

Lipford et al. (Lipford, Besmer et al. 2008) introduisent et évaluent l'interface de l'audience d'un profil. Ce système permet à un utilisateur d'afficher son profil tel qu'il apparaît à un ami ou à un groupe d'amis. Une variante de cette interface est actuellement appliquée par Facebook. L'utilisation d'interfaces de réseaux extensibles a été suggérée par Reeder et al.(Reeder, Bauer et al. 2008). Leur système permet à un administrateur système de visualiser et de modifier les paramètres de contrôle d'accès à son profil.

Adu-Oppong et al. et Danezis et al. (Adu-Oppong, Gardiner et al. 2008; Danezis 2009) proposent de nouvelles interfaces utilisateurs pour spécifier les paramètres de la vie privée des réseaux sociaux par le groupement d'amis de l'utilisateur dans des listes basées sur les communautés extraites automatiquement du réseau. Cependant, ils n'ont pas étudié les préférences de confidentialité des utilisateurs réels pour évaluer leur

proposition. Dans les deux cas, les outils proposés sont basés sur le partitionnement des amis dans un ensemble fixe de non-chevauchement des communautés.

Dans le même principe, certaines études (Maximilien, Grandison et al. 2009; Liu and Terzi 2010) proposent une méthodologie pour quantifier le risque posé par les paramètres de confidentialité d'un utilisateur. Un score de risque révèle à l'utilisateur dans quelle mesure ses paramètres de confidentialité son accessible à d'autres utilisateurs. Il lui fournit des critiques générales sur ses paramètres et comment elles sont appliquées chez d'autres personnes. Cependant, il ne l'aide pas à mettre en place une politique initiale et à raffiner ses réglages afin de parvenir à une configuration plus sûre.

D'autre part, Carmagnola et al. (Carmagnola, Verner et al. 2009) présentent SONARS, un nouveau algorithme pour recommander du contenu dans les systèmes de recommandation sociaux. SONARS cible les utilisateurs en tant que membres de réseaux sociaux, en suggérant des paramètres qui reflètent la tendance du réseau lui-même, basé sur sa structure et sur les relations entre les utilisateurs. Ma et al. (Ma, Zhou et al. 2011) se concentrent sur le problème de la recommandation sociale. Ils proposent deux algorithmes de recommandation sociale en se basant sur l'intuition que les informations des amis de l'utilisateur peuvent apporter pour améliorer la précision de la prédiction des systèmes de recommandation.

Les études citées précédemment sont divisées en deux grands groupes. Des études qui ont traité le vol d'identité comme phénomène en montrant les risques qu'encourent les utilisateurs quand ils ne protègent pas leurs données privées. Ces études sont importantes pour Protect-U puisqu'il se base sur des recommandations qui demandent des études statistiques sur les comportements des utilisateurs.

Ensuite il y a les études qui essayent de proposer des solutions à ces risques que ce soit en recommandant des conseils aux utilisateurs ou bien en changeant automatiquement leurs paramètres.

Nous allons présenter dans ce qui suit ces deux groupes.

## 4.2 Études sur les risques

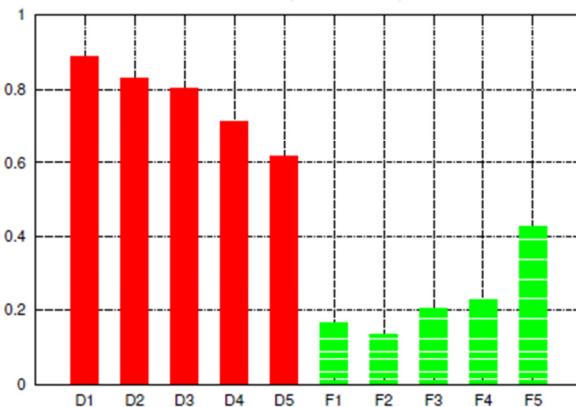
Fogel et al. (Fogel and Nehmad) ont étudié les risques d'atteinte à la vie privée sur les réseaux sociaux. Ils ont pris 205 étudiants de niveau collégial en étudiant leur comportement et leur conscience sur les dangers des réseaux sociaux. Ils ont conclu que les personnes qui ont un profil sur un réseau social sont plus à risque concernant leur vie privée que les autres. Ce phénomène est plus grand chez les hommes que chez les femmes. Ils ont noté plusieurs autres faits :

- Les hommes sont plus à risque que les femmes par rapport à la protection de leur vie privée.
- Les préoccupations de divulgation des renseignements privés sont plus grandes chez les femmes que chez les hommes.
- Les hommes affichent plus leurs numéros de téléphones et adresses de domicile sur les réseaux sociaux que les femmes. Au total, les auteurs ont trouvé que 10% des participants ont affiché leurs numéros de téléphone. Ils ont observé le même taux pour l'adresse.
- Les femmes écrivent plus de commentaires sur les murs des autres personnes et expriment plus leurs sentiments que les hommes.
- Les hommes ont plus d'amis sur leurs comptes que les femmes. En effet les femmes sont souvent plus sélectives dans le choix de leurs contacts. Elles acceptent moins d'étrangers.
- Les utilisateurs de Facebook ont un plus grand sentiment de confiance que ceux de MySpace.
- La plupart des participants ont exprimé leur besoin d'être informés des risques d'utilisation de ces sites sur leurs vies privées avant l'inscription.

Bilge et al. (Bilge, Strufe et al.) ont étudié les techniques d'attaque et de vol d'identité à travers les réseaux sociaux. En l'occurrence par quels moyens un attaquant peut-il lancer des attaques automatiques d'usurpation d'identité afin de collecter le maximum d'informations personnelles des utilisateurs de certains réseaux sociaux. Deux attaques ont été décrites dans l'étude :

La création de profils fictifs correspondant à des utilisateurs réels. Puis l'envoi automatique d'invitation à leurs amis. Les amis pensant que leur ami a créé un nouveau compte acceptent l'invitation, l'attaquant peut alors récupérer des informations sensibles du profil de la victime.

La figure 17 présente leur résultat.



**Figure 17: Pourcentage d'acceptation des demandes d'ajout**

(D1 ... D5) représentent le pourcentage d'acceptation de demande d'ajout d'un profil usurpé. Malgré le fait que les amis ont déjà le profil de la personne usurpé dans leurs listes de contacts, ils ont quand même accepté l'ajout. Ce pourcentage arrive à 90% pour le profil D1.

(F1 ... F5) représentent le pourcentage d'acceptation de demande d'ajout d'un profil fictifs. Le pourcentage est moins fort que le premier groupe, mais il arrive à 40% pour F5.

La deuxième attaque étudiée est l'envoi automatique de demandes d'ajout d'amis sur des sites de réseaux sociaux ou la victime ne s'est pas encore inscrite. Les auteurs cherchent les amis de la victime qui sont inscrits sur des réseaux sociaux ou la victime n'est pas encore inscrite. Crée un profil usurpé sur ces réseaux et invite ses amis. Le tableau 2 présente les résultats :

**Tableau 2: Pourcentages des profils Xing trouvés sur LinkedIn**

Profiles	Xing	LinkedIn
X1	18.2%	50.0%
X2	14.5%	66.6%
X3	22.8%	51.6%
X4	14.5%	100.0%
X5	15.6%	46.4%
Total	17.6%	56.4%

Le pourcentage d'acceptation d'une demande d'ajout d'amis est très grand lorsque la victime connaît la personne usurpé, mais que la demande est faite sur un autre réseau social.

Brown et al. (Brown, Howe et al.) ont basé leur étude sur les courriels électroniques frauduleux dans les réseaux sociaux. Les courriels électroniques sont l'un des moyens les plus utilisés par les attaques sur internet tel que le phishing, les spamming ... Plusieurs techniques ont été mises au point pour contrer ces attaques. Ils ont cité comme exemple MessageLabs qui scanne des millions de courriels par jour et signalent tout courriel suspecté de contenir un logiciel malveillant. Ces techniques pour détecter les courriels infectés sont tellement efficaces que les attaques à partir des courriels se sont adaptées. Ils dépendent maintenant entièrement des internautes qui doivent cliquer sur un lien pouvant les mener vers un site infecté. Cette nouvelle technique a rendu la détection de l'infection difficile par les logiciels de protections. Pour masquer la nature du courriel malveillant, les pirates utilisent plusieurs méthodes : ils changent l'entête du courriel, utilisent des images réactives ou encore imitent des courriels envoyés par des sites commerciaux connus. Une autre méthode proposée par les auteurs consiste à créer des courriels contenant des informations privées des amis de la victime sur les réseaux

sociaux. Dans le but d'induire la victime en erreur en lui faisant croire que c'est un courriel envoyé par l'un de ses amis.

Les auteurs ont analysé les attaques qui impliquent l'utilisation des messages électroniques et exploitent les caractéristiques des réseaux sociaux tel que le partage d'information entre les amis, et surtout les informations personnelles des amis comme la date d'anniversaire, la ville d'origine ou les évènements communs. Ces informations renforcent l'authenticité des courriels et donnent confiance aux utilisateurs pour qu'ils cliquent sur des liens pouvant les mener vers des logiciels malveillants.

Ils ont analysé dans leur étude 7000 profils Facebook d'étudiants de l'université de Michigan. Ils ont déterminé trois attaques possibles :

**-Attaque basée sur la relation** : cette attaque utilise seulement les renseignements partagés entre les deux amis.

**-Attaque basée sur les informations non en commun** : elle utilise seulement l'attribut d'une des deux parties. Comme la date d'anniversaire de l'un des deux amis par exemple.

**- Attaque basée sur les informations en commun** : elle utilise les attributs visibles en commun entre deux amis comme la ville natale commune.

Pour chacune de ces trois attaques, ils ont créé un modèle de courrier électronique.

Plusieurs observations ont été faites lors de cette étude. Les utilisateurs avec des profils fermés sont vulnérables aux attaques parce que leurs amis ont des profils ouverts. La plupart des utilisateurs qui ont participé à cette étude ont un grand nombre d'amis, supérieur à 300. Ce qui rend plus probable que l'attaquant trouve l'un de ces amis avec un compte ouvert qui pourra le mener aux informations de l'utilisateur testé.

Sur les 7000 utilisateurs visés par l'étude, 905 ont des profils amis ouverts qui existent aussi dans le spécimen d'étude. Les auteurs ont trouvé que 24% d'entre eux étaient

vulnérables à une attaque visant la ville natale et 4% à une attaque visant les évènements en commun avec ces profils ouverts.

### 4.3 Solutions proposées

Fang, L. et K. LeFevre (Fang and LeFevre) proposent un assistant de protection à la vie privée dans les réseaux sociaux. Cela se fait par la construction d'un modèle d'apprentissage machine à partir de quantité limité de données personnelles des utilisateurs. Il règle automatiquement les paramètres de confidentialités de ces utilisateurs.

L'assistant demande à l'utilisateur de manière interactive d'affecter des notes à un groupe d'amis choisi aléatoirement. Il va utiliser cette entrée pour construire un classifieur qui peut être utilisé pour attribuer automatiquement des priviléges à l'ensemble des autres utilisateurs.

Pour évaluer cette approche, les auteurs ont recueilli les données privées de 45 participants sur Facebook. À chaque utilisateur, deux types de questions lui sont posés. En première étape, un ensemble de données privées les plus représentatives d'un profil Facebook ont été sélectionnées tel que la date de naissance, l'adresse, l'opinion politique... L'utilisateur devra pour chaque donnée spécifier le niveau de partage de cette information avec ses contacts. Ensuite vérifier les groupes de personnes qui peuvent la voir.

Un imprimé-écran du premier test est affiché dans la figure 18.

<b>date_of_birth</b>	<input checked="" type="radio"/> All friends	<input type="radio"/> Some of my friends	<input type="radio"/> No one
<b>home_address</b>	<input checked="" type="radio"/> All friends	<input type="radio"/> Some of my friends	<input type="radio"/> No one
<b>relationship_status</b>	<input type="radio"/> All friends	<input checked="" type="radio"/> Some of my friends	<input type="radio"/> No one
<b>photos</b>	<input type="radio"/> All friends	<input checked="" type="radio"/> Some of my friends	<input type="radio"/> No one
<b>political_view</b>	<input type="radio"/> All friends	<input checked="" type="radio"/> Some of my friends	<input type="radio"/> No one
<b>religious_view</b>	<input type="radio"/> All friends	<input checked="" type="radio"/> Some of my friends	<input type="radio"/> No one
<b>status_update</b>	<input type="radio"/> All friends	<input checked="" type="radio"/> Some of my friends	<input type="radio"/> No one

[Submit](#)

**Figure 18 : Imprime écran de questions posées à l'utilisateur**

Le second questionnaire collecte plus de détails sur ces réponses. L'utilisateur doit sélectionner les personnes qui peuvent voir chacune des données privées qu'il a spécifiées accessibles à un certain groupe d'amis.

Un imprimé-écran du deuxième test est affiché dans la figure 19.

**Figure 19:** Imprime écran d'une question détaillée posée à l'utilisateur

Après avoir collecté toutes ces données, les auteurs ont appliqué divers techniques d'apprentissage machine et ils ont déduit un modèle de préférence qui classe le réseau d'amis en des groupes de confiance en prenant en compte plusieurs données comme l'appartenance communautaire de ces amis.

Cette étude a révélé les utilisateurs des réseaux sociaux ont tendance à donner des droits d'accès à leurs amis en termes de communautés tels que des amis d'étude, des amis de travail, famille proche.

Mazzia, A.L.K. et E. Adar (Mazzia and Adar) introduisent PViz un système qui permet à l'utilisateur de comprendre la visibilité de son profil en fonction de la nature de ses sous-groupes d'amis. Il se base sur une interface graphique qui représente le réseau d'amis de l'utilisateur sous forme de nœuds. Chaque noeud englobe les amis appartenant à un sou- groupe défini par une certaine sémantique. Le système permet aussi de sélectionner la liste de données personnelles que l'utilisateur peut configurer pour rendre son profil plus confidentiel.

Les auteurs de PViz ont basé leur étude sur 20 participants d'un âge moyen de 23 ans. Tous les participants sont abonnés depuis au moins un an et étudient dans la même université. Ces participants ont répondu à 36 questions divisées en deux groupes. Questions personnelles : exemple « Est-ce que tu peux voir la date de naissance de ton amie Alice ? ». Et des questions de groupes dans laquelle une même question est posée à plusieurs personnes « Est-ce que tout le groupe peut voir les mises à jour du statut de Margaret ? ». Dépendamment de la réponse aux questions, un ensemble de remarques sont générées pour chacun des amis du participant qui ont participé eux aussi au test. Ces remarques décrivent le comportement des amis testés sur Facebook. Les utilisateurs finiront par répondre à trois questions :

- Cet outil m'a aidé à comprendre les paramètres de la vie privée de mes amis.
- J'ai aimé utiliser cet outil.
- Je veux utiliser cet outil sur mon propre profil Facebook.

Lipford et al. (Lipford, Besmer et al.) ont développé *Audience View*, un outil qui examine la vie privée dans les réseaux sociaux. Il vise à améliorer la sécurité de la vie privée et aide à la gestion des accès pour les renseignements personnels.

Dans leur article ils ont comparé l'interface de paramétrage des données personnelles qu'offre Facebook avec leur prototype d'interface pour voir quelle interface protège le mieux la vie privée. Les participants au test ont interagi avec une même personne abonnée à Facebook et différentes personnes utilisant l'interface Audience View.

La figure suivante donne un aperçu sur le prototype d'interface Audience View.



Figure 20: Audience View interface

L'ordre d'utilisation des interfaces était aléatoire. À la fin du test, les participants ont répondu à cinq questions différentes sur ces paramètres de confidentialité et ils ont déterminé qui a eu accès à quelles informations personnelles.

Les auteurs ont demandé aux participants d'indiquer comment ils étaient à l'aise avec l'utilisation de chaque interface. Un exemple de question posée : Si une personne était à la recherche d'une autre personne qui n'est pas son ami, serait-il en mesure d'obtenir les informations suivantes de son profil :

Le nom, l'image de profil, l'adresse courriel, la date d'anniversaire.

Seize personnes ont participé à l'étude, 7 femmes et 9 hommes. 63% des participants avaient déjà utilisé Facebook.

Plusieurs faits ont été observés lors de leur test. Les utilisateurs de Facebook ont de la difficulté à comprendre les paramètres de confidentialité existante. Ils préfèrent visualiser le résultat de changement des paramètres plutôt que simplement lire les

descriptions. Facebook demande à l'utilisateur de se familiariser avec l'interface et de connaitre la structure de son réseau pour comprendre l'impact potentiel des paramètres de confidentialités sur ses amis. Par contre ce système offre à l'utilisateur la possibilité de voir les paramètres et le groupe d'amis correspondant dans la même interface.

Alors que beaucoup de travaux ont mis l'accent sur les outils pour comprendre et régler les paramètres de confidentialité existants, Protect\_U (Hélou, Gandouz et al. 2012) utiliser des techniques d'apprentissage machine pour recommander les paramètres de confidentialité à l'utilisateur avec le minimum de contribution de sa part.

Protect\_U analyse le contenu des profils utilisateurs et les classes en fonction de quatre niveaux de risques : risque faible, risque moyen, risqué et critique. Le système propose ensuite des recommandations personnalisées pour permettre aux utilisateurs de rendre leurs comptes plus sûr. Pour ce faire, il s'appuie sur deux modules de protections : locale et communautaire. Le premier module utilise les données personnelles de l'utilisateur afin de proposer des recommandations appropriées. Il appartient à l'utilisateur d'accepter ou de rejeter ces recommandations. Le second modèle cherche des amis dignes de confiance de l'utilisateur pour les encourager à contribuer à l'amélioration de la sécurité de ce compte.

## Chapitre 5 : Conception et méthodologie

Au cours de ce chapitre, nous allons présenter notre approche, décrire l'architecture de notre système *Protect\_U* (Hélou, Gandouz et al. 2012) et expliquer la méthodologie adaptée pour répondre à nos besoins.

Nous avons développé un système de protection de la vie privée des utilisateurs de Facebook appelé *Protect\_U*. Notre choix s'est porté sur Facebook parce qu'il contient le plus grand nombre d'utilisateurs, comparé à d'autres réseaux sociaux.

Pour protéger les utilisateurs, *Protect\_U* a besoin de collecter un certain nombre de leurs données personnelles.

Facebook permet aux utilisateurs d'insérer une très grande quantité d'informations. Dans ce qui suit la liste des données accessible sur un profil. Elles sont divisées en 6 groupes :

**Mur:** cet endroit recense toutes les publications qui peuvent être du texte, des photos, des publications d'autres groupes, des activités, des vidéos postées par d'autres personnes, des formations et emplois.

**Informations:** cet endroit regroupe toutes les informations personnelles comme le sexe, la date de naissance, la ville de naissance, la ville actuelle, les groupes et pages auxquelles l'utilisateur est abonné, la formation, l'emploi, les films préférés, les livres préférés, les citations favorites.

**Photos :** ce groupe contient les photos et albums que l'utilisateur a publiés. Il contient aussi les photos dans lesquelles il est tagué. Les images taguées sont celles qui n'appartiennent pas forcément à l'utilisateur, mais plutôt à l'un de ses amis qui l'a marqué dedans.

**Aperçu :** cette section regroupe les applications installées par l'utilisateur et les raccourcis pour les groupes de discussions.

**Vidéos**: cet endroit regroupe les vidéos enregistrées par l'utilisateur ou bien dans lesquelles il est tagué.

**Boite de réception**: cet endroit regroupe tous les messages envoyés et reçus par l'utilisateur. Dès le début de 2012, les discutions instantanées ont été ajouté à ce groupe.

Ninggal et Abawajy (Ninggal and Abawajy 2011) ont limité ces données à un groupe plus restreint, en éliminant les données qui ne reflètent pas la personnalité de l'utilisateur ou bien qui donne des informations vagues sur lui. Les données spécifiés par Ninggal et Abawajy et prises en compte par Protect-U sont : l'*âge*, le *sexe*, le *nombre d'amis*, le *nombre de publications par semaine*, le *nombre de groupes auxquels il est inscrit*, le *nombre total d'images* (privées et publiques), le *pourcentage d'images privées dans son compte* et des données sensibles comme la *religion* et la *position politique*. Ces paramètres sont importants parce que groupés, ils peuvent révéler la surexposition des utilisateurs aux dangers des réseaux sociaux. Les valeurs de ces paramètres sont stockées dans la base de données *Archive utilisateurs* (voir Figure 21). Un exemple de ces paramètres est illustré par le tableau 3.

**Tableau 3 : Aperçu de quelques profils de participants**

Age	Gender	Number of friends	Number of publications per week	Number of groups	Number of pictures	Percentage of private pictures	Sensitive data
23	Male	112	13.46	268	43	0	Yes
15	Female	115	19.44	80	194	0	Yes
22	Female	122	12.5	31	60	0	No
28	Female	124	21.88	165	383	98.96	yes

Les données récoltées à ce niveau serviront d'entrée pour les deux modules que constitue *Protect\_U* : le *module de classification* et le *module de recommandations*.

L'architecture générale du système est représentée à la figure 21.

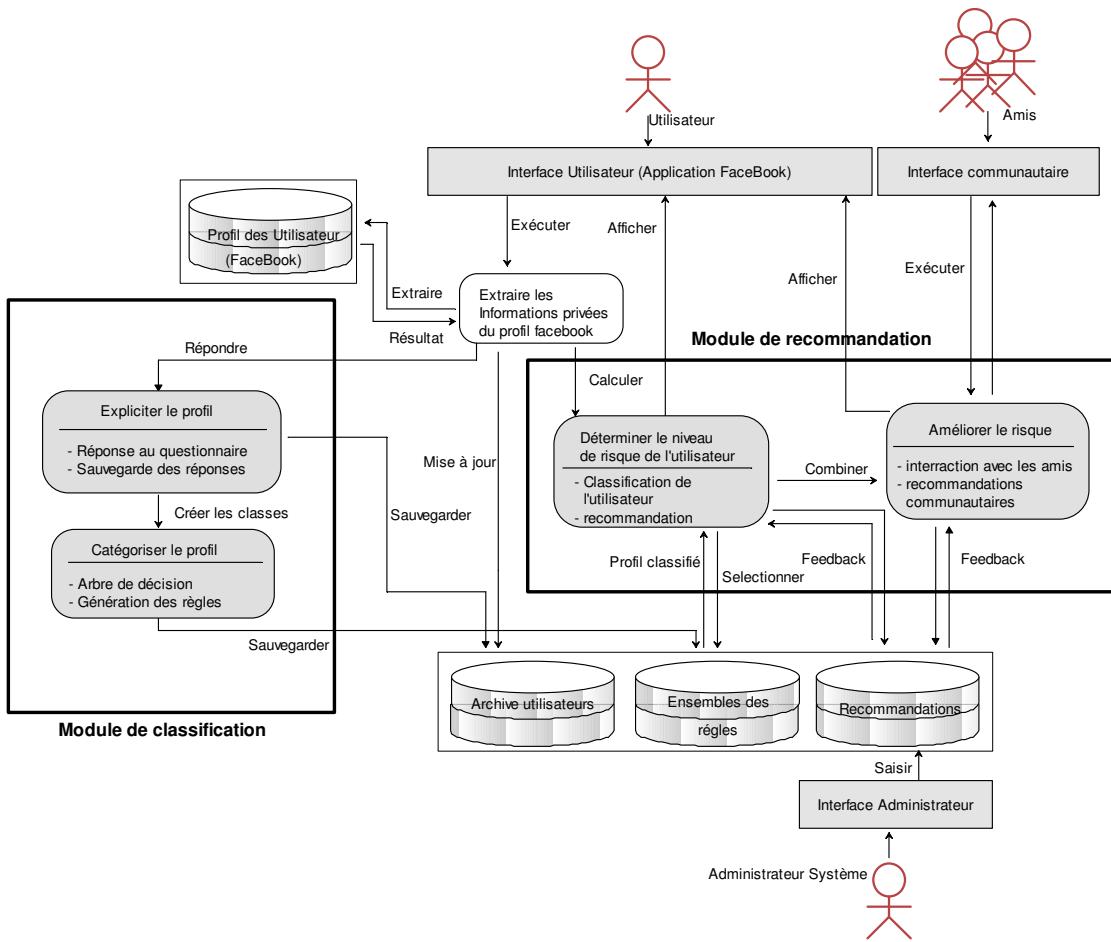


Figure 21 : Architecture de Protect\_U

## 5.1 Module de classification

Le *module de classification* se compose de deux étapes :

### 5.1.1 Expliciter le profil

La première étape « *Expliciter le profil* » consiste à afficher aux participants un questionnaire contenant 18 questions portant sur diverses atteintes à la vie privée sur Facebook. Pour créer ce questionnaire, nous nous sommes appuyé sur une étude menée par Statistique Canada en 2009 (Canada 2009). Cette enquête est faite sur un questionnaire constitué de 210 questions liées à la vie privée. En nous basant sur l'étude d'Aïmeur et al. (Aïmeur, Gambs et al. 2010), nous avons divisé les niveaux d'atteinte à

la vie privée de ces questions en quatre classes : *peu risquée*, *moyennement risquée*, *risquée* et *critique*.

Ces 18 questions sont divisées en trois groupes correspondants aux quatre classes les plus risquées citées ci-dessus. Les questions du *groupe 1* sont associées à la classe *moyennement risquée*. Il s'agit de questions qui permettent de déterminer si l'utilisateur possède des informations sensibles dans son compte qui ne causent pas de danger dans l'immédiat, mais leur cumul pourrait lui nuire. La figure 22 donne un exemple de question de ce groupe.

**3- Comment affichez-vous votre date de naissance ?**

- Au complet
- Mois et jour seulement
- Cachée

**Figure 22 : Question liée aux profils moyennement risqués**

Les questions du *groupe 2* sont associées à la classe *risquée*. Il s'agit de questions qui permettent de déterminer si l'utilisateur a eu des ennuis à cause des informations affichées sur Facebook. Voir figure 23

**10- Avez-vous reçu des commentaires indécents sur votre mur ou dans une de vos publications ?**

- Oui
- Non

**Figure 23 : Question liée aux profils risqués**

Les questions du *groupe 3* sont associées à la classe *critique*. Il s'agit de questions qui permettent de déterminer si l'utilisateur a déjà subi un harcèlement physique ou moral suite à la publication d'un contenu dérangeant, ou s'il a publié une information sensible pouvant mettre sa vie privée en danger. Voir figure 24.

**17- Avez-vous été confronté à un harcèlement de la part d'un autre membre ?**

- Oui
- Non

**Figure 24 : Question liée aux profils critiqués**

Nous avons affecté à chaque participant la classe correspondant au niveau de risque le plus élevé selon ses réponses au questionnaire. Les profils des participants ont ainsi été classés en quatre classes:

- 1- Profil *peu risqué* (*low risk*) si un participant a répondu « non » à toutes les questions.
- 2- Profil *moyennement risqué* (*medium risk*) si un participant a répondu « oui » à au moins une des questions du *groupe 1*.
- 3- Profil *risqué* (*risky*) si un participant a répondu « oui » à au moins une des questions du *groupe 2*.
- 4- Profil *critique* (*critical*) si un participant a répondu « oui » à au moins une des questions du *groupe 3*.

Le tableau 4 présente un exemple de classification de participants. Le niveau de risque du premier utilisateur a été considéré de niveau *risqué* parce qu'il a répondu « oui » à la question « Affichez-vous votre numéro de téléphone ou votre adresse dans votre profile Facebook ? » qui est classé question de niveau *risqué*.

**Tableau 4 : Affection des niveaux de risques aux utilisateurs**

Age	Gender	Number of friends	Number of publications per week	Number of groups	Number of pictures	Percentage of private pictures	Sensitive data	Level of risk
23	Male	112	13.46	268	43	0	Yes	Risky
15	Female	115	19.44	80	194	0	Yes	Critical
22	Female	122	12.5	31	60	0	No	Critical
28	Female	124	21.88	165	383	98.96	Yes	Risky

### 5.1.2 Catégoriser le profil

La deuxième étape (*Catégoriser le profile*) consiste à appliquer la technique des *arbres de décisions* (Kantardzic 2011) pour pouvoir extraire des *règles de classification*. Chaque chemin de cet arbre constitue une règle associée à une classe. Ces règles sont sauvegardées dans la base de données *Ensemble des règles* (figure 27). L'avantage des arbres de décision est leur performance et la grande lisibilité de leur forme arborescente. Généralement, *ID3* et *C4.5* (Soman, Diwakar et al. 2006) sont les algorithmes les plus utilisés dans les arbres de décision. C4.5 a été retenu vu ses nombreux avantages face à

*ID3* notamment lors du traitement simultané des attributs continus et discrets, ainsi que les données avec attributs manquants. La figure 25 illustre un exemple de règle obtenue suite à l'application de l'arbre de décision. Elle est interprétée comme suit : « Si le nombre d'images est inférieur ou égal à 256, le nombre d'amis est supérieur strictement à 102.5, le nombre de publications par semaine est strictement supérieur à 10.33 et le sexe est masculin alors le profil est risqué ».

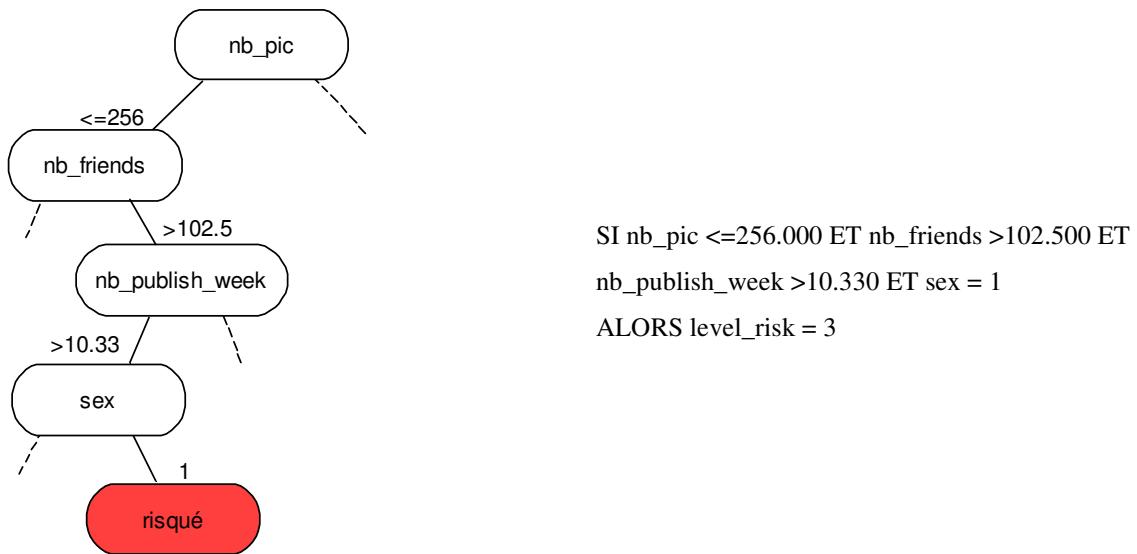


Figure 25 : Exemple d'extraction de scénarios

Pour valider les performances de l'algorithme, la méthode de *validation croisée (Cross-validation)* « *leave-one-out* » a été appliquée. Cette méthode s'adapte le mieux au cas où le nombre de données d'apprentissage n'est pas très élevé. C'est un cas particulier de la méthode *K-fold cross-validation* qui divise aléatoirement l'échantillon initial des données d'apprentissage en *k* sous-ensembles. Elle utilise les *k-1* premiers sous-ensembles pour construire le modèle et le valide avec le sous-ensemble restant. La méthode *leave-one-out* applique la même procédure à l'exception que *K* représente le nombre total des participants de l'échantillon initial (Bramer 2007).

Une fois les *règles de classification* spécifiées, un *ensemble de recommandations* est créé et saisi par un administrateur en tenant compte des conditions et des seuils générés

par l'application de l'arbre de décision. Cet ensemble de recommandations est stocké dans la base *Recommandations*.

## 5.2 Module de recommandation

Lorsqu'un utilisateur exécute l'application, *Protect\_U* récolte ses *données personnelles*, ses *données démographiques* (*âge*, *nationalité* et *situation familiale*) ainsi que la *liste des noms de ses amis*.

Le *module de recommandations* utilise ces informations récoltées pour proposer des recommandations adaptées aux profils des utilisateurs et les inciter à mieux se protéger. Pour ce faire, il applique deux filtres : le *Filtre à base de connaissances* et le *Filtre communautaire*. L'architecture générale du *module de recommandation* est illustrée par la figure 26.

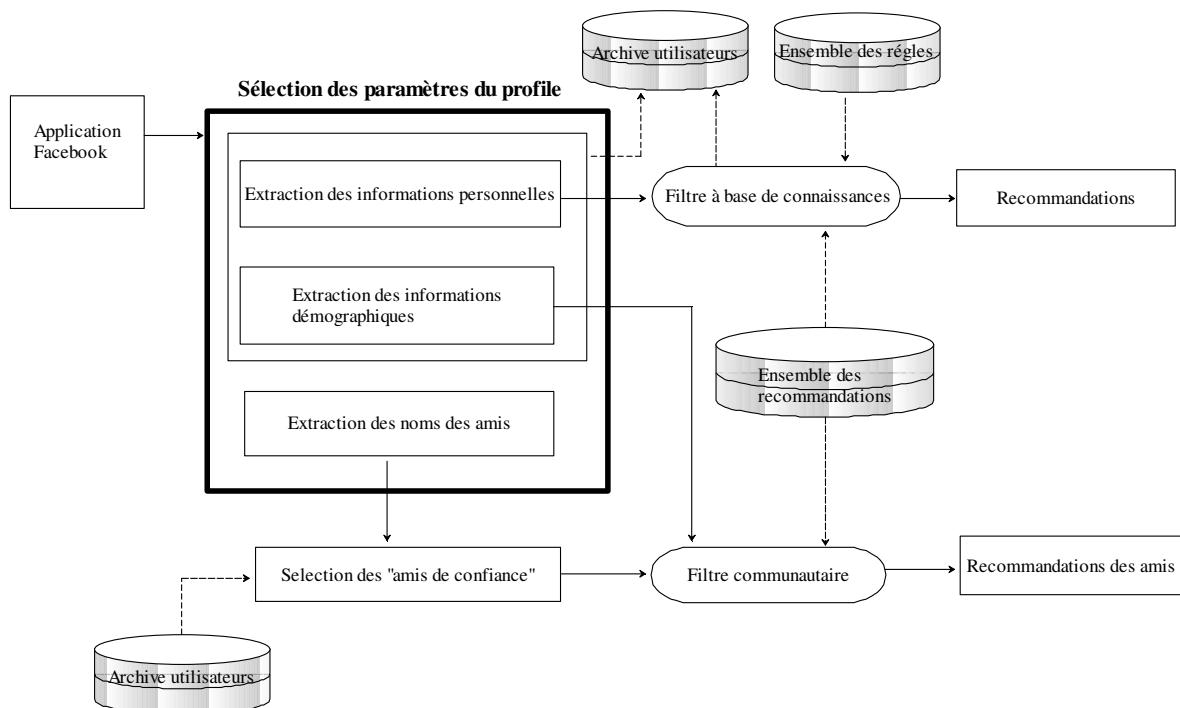


Figure 26. Recommandation module

### 5.2.1 Filtre à base de connaissances

Le *Filtre à base de connaissances* utilise les *données personnelles* des utilisateurs et les *règles* stockées dans la base de données *ensemble des règles* pour déterminer la classe du profil de l'utilisateur et les recommandations appropriées. Il utilise la règle la plus proche du profil en appliquant la *fonction de similitude vectorielle*. Pour un profil A et une règle B, la *fonction de similitude* est donnée par la formule 1:

$$\text{cosinus } (A, B) = \sum_{i=1}^N \frac{v_{A,i}}{\sqrt{\sum_{i=1}^N v_{A,i}^2}} * \frac{v_{B,i}}{\sqrt{\sum_{i=1}^N v_{B,i}^2}} \quad (\text{Formule 1})$$

N étant le nombre maximal de paramètres considérés,  $v_{A,i}$  la valeur du paramètre i de l'utilisateur A et  $v_{B,i}$  la valeur du paramètre i de la règle B. La règle qui donne le plus petit angle du  $\cos(A, B)$  sera affectée au profil A.

#### Exemple 1 :

Supposons qu'on cherche à trouver la règle qui correspond le plus au profil d'un utilisateur A ayant les paramètres suivants :

$v_{A,1} = \hat{\text{Age}} = 15$ ,  $v_{A,2} = \text{Nombre d'images publiées} = 300$ ,  $v_{A,3} = \text{Nombre d'amis} = 1200$ .

Supposons aussi qu'on dispose des trois règles suivantes :

Règle B1 : si  $v_{B1,1} < 18$ ,  $v_{B1,2} > 100$  et  $v_{B1,3} > 50$  alors profil *risqué*

Règle B2 : si  $v_{B2,1} > 40$ ,  $v_{B2,2} < 20$  et  $v_{B2,3} < 10$  alors profil *peu risqué*

Règle B3 : si  $v_{B3,1} < 25$ ,  $v_{B3,2} > 30$  et  $v_{B3,3} > 100$  alors profil *risqué*

Le profil de l'utilisateur vérifie les règles B1 et B3. Le cosinus le plus élevé (ou l'angle le plus petit) détermine laquelle de ces deux règles est plus proche de son profil. Puisque  $\cos(A, B1) = 0.644$  et  $\cos(A, B3) = 0.97$  on peut déduire que le profil de l'utilisateur A est plus proche de la règle B3 et ce qui correspond à un profil *critique*.

Une fois la règle la plus proche du profil de l'utilisateur est déterminée, le *Filtre à base de connaissances* va fouiller la base de données *ensemble des recommandations* pour trouver les recommandations qui vérifient les conditions imposées par cette règle. À titre d'exemple, la règle représentée dans la figure 25 associée à un profil risqué donne la recommandation suivante :

**« Réduisez le nombre de publications affichées sur votre mur.** Un grand nombre d'informations publiées sur votre mur augmente le risque de récolte de renseignements personnels de votre profil. Faites attention au contenu de ce que vous partagez, pensez toujours qu'il y a des amis qui pourraient être affectés ou dérangés par le contenu des vidéos ou images que vous publiez. Cela pourrait affecter votre relation avec eux. »

### 5.2.2 Filtre communautaire

Le *Filtre communautaire* cherche à améliorer la qualité des recommandations en faisant appel au réseau d'amis de l'utilisateur. Pour cela, *Protect\_U* favorise les *amis de confiance* qui connaissent mieux l'utilisateur. Un *ami de confiance* est un ami appartenant à l'un des groupes suivants :

- *Membres de la famille.*
- *Amis proches.*
- *Personnes avec qui l'utilisateur communique le plus.*
- *Personnes « taguées » dans les images affichées dans le profil de l'utilisateur.*

En répondant à un questionnaire, ces amis contribuent à raffiner les informations déjà récoltées sur l'utilisateur et à cibler les faiblesses de son profil. Le questionnaire vise essentiellement à connaître le niveau de risque en tenant compte des éléments suivants : le *contenu des images affichées*, le *contenu des commentaires* et *celui des publications* (vidéo, liens externes, etc.). Les questions posées sont choisies en fonction des informations récoltées à partir de la *sélection démographique* (*âge*, *nationalité* et

*situation familiale*). Ainsi, les questions posées à un adulte seront différentes de celles posées à un mineur.

D'un autre côté, le système vérifie si les amis ont déjà exécuté *Protect\_U* en vérifiant si la base de données *Archive utilisateurs* détient déjà le niveau de risque de leurs profils. Si oui, leurs niveaux de risque seront pris en considération dans le calcul des amis de confiance (voir figure 26).

Pour sélectionner les *amis de confiance*, on affecte une valeur notée *Poids* (voir formule 2), à chacun des amis de l'utilisateur. Ce poids dépend des paramètres suivants : le *lien de connaissance* avec l'utilisateur ( $C_1$ ), le *nombre de messages échangés avec l'utilisateur* ( $C_2$ ), le *nombre de fois que l'ami est tagué dans le compte de l'utilisateur* ( $C_3$ ) et le *niveau de risque du profil de l'ami* ( $C_4$ ).

Il est primordial de signaler que, pour les différents variables et coefficients mentionnés dans cette section, plusieurs essais étaient nécessaires pour trouver des valeurs pertinentes menant à de bons résultats.

Si le *niveau de risque* de l'ami est connu,  $C_4$  prendra la valeur 2 pour un profil *peu risqué*, 1.5 pour un profil *moyennement risqué*, 0.5 pour un profil *risqué* ou 0 pour un profil *critique*. La valeur zéro veut dire que dans le cas d'un profil critique, l'ami en question sera écarté de la liste des amis de confiance. Dans le cas où *Protect\_U* n'est pas en mesure de déterminer le niveau de risque de l'ami, il affectera 1 à  $C_4$ . Ce qui veut dire que ce paramètre ne sera plus pris en considération. Ainsi  $C_4$  appartient à l'intervalle {0, 0.5, 1, 1.5, 2}.

Pour donner un plus grand poids aux paramètres selon leur ordre d'importance, nous avons affecté la valeur 3 au *lien de connaissance*, la valeur 2 au *nombre de messages échangés* et 1 au *nombre de fois qu'il est tagué*. Avec ces valeurs, la priorité a été donnée aux usagers qui font partie des *membres de la famille* ou de la liste des *amis proches* parce qu'on considère qu'ils connaissent mieux l'utilisateur. D'un autre côté, un ami qui échange beaucoup de messages avec l'utilisateur est censé le connaître sans forcément être dans sa liste de « liens de connaissance ». En troisième lieu, il arrive

qu'une personne taguée sur une photo de l'utilisateur soit proche de lui. D'où la fonction :

$$P(C_i) = \begin{cases} 3 & \text{si } i = 1 \\ 2 & \text{si } i = 2 \\ 1 & \text{si } i = 3 \end{cases}$$

Ensuite, une pondération  $\alpha_i$  a été affectée à chaque paramètre  $C_i$  (i varie entre 1 et 3) afin de raffiner la pondération générale.  $\alpha_1$  prend la valeur 2 si l'ami est un membre de la famille, 1 s'il est un ami proche et zéro dans les autres cas.  $\alpha_2$  est la partie entière de  $\frac{3 * C_2}{MAX}$  (Max étant le nombre maximal de messages échangés par tous les amis).  $\alpha_3$  est la partie entière de  $\frac{3 * C_3}{TAG}$  (TAG étant le nombre maximal d'images où l'utilisateur est tagué). Ainsi,  $\alpha_1 \in \{0, 1, 2\}$ ,  $\alpha_2 \in \{0, 1, 2, 3\}$  et  $\alpha_3 \in \{0, 1, 2\}$ .

Par conséquent, les poids sont calculés à partir de la formule 2 suivante :

$$\text{Poids} = C4 \sum_{i=1}^3 \alpha_i P(C_i) \quad (\text{Formule 2})$$

### **Exemple 2 :**

Considérons un ami qui fait partie des membres de la famille de l'utilisateur à protéger. On suppose qu'ils ont échangé 20 messages et que le nombre de messages total échangés entre l'utilisateur et ses amis est de 300. On suppose aussi que son profil a été tagué 7 fois par l'utilisateur sur un total de 10 images taguées. De plus, Protect\_U a trouvé que le profil de son compte est moyennement risqué.

Le poids que la formule 2 accorde à cet ami est donné par ce qui suit:  $1.5 (2*3 + 0*2 + 2*1) = 12$ .

De cette façon, Protect\_U affecte à chaque ami un poids et seuls les 10 amis qui ont obtenu les plus grands poids sont retenus comme « amis de confiance ».

Notons que *Protect\_U* donne aussi la possibilité à l'utilisateur de *modifier lui-même* la liste de ses amis de confiance. Ceci est important dans la mesure où l'utilisateur préfère parfois ajouter des amis ne figurant pas dans la liste générée par *Protect\_U*.

La dernière étape consiste à envoyer à l'utilisateur le niveau de risque de son profil et les recommandations associées.

Dans la section suivante, nous présentons les détails de l'implémentation de *Protect\_U* ainsi que les résultats de sa validation.

# Chapitre 6 : Implémentation et validation

*Protect\_U* a été développé avec la plateforme de Facebook (Facebook SDK) permettant l’interaction entre les utilisateurs et le système. Cette plateforme fournit des fonctionnalités coté serveur très riches donnant accès aux *fonctions de réseautage*, aux *informations partagées* et à la *liste des amis des utilisateurs*.

Nous avons utilisé la technologie PHP et Javascript pour implémenter PROTECT\_U. Notre choix résulte du fait que Facebook fournit une API (Application programming interface) développée avec cette technologie permettant d'accéder aux informations des profils des utilisateurs. A noter que la condition nécessaire pour récolter ces informations est l'autorisation préalable de l'utilisateur du système.

La section suivante présente les *prédictions* obtenues au niveau du *module de classification* ainsi que les résultats de la *validation du module de recommandation*.

## 6.1 Module de classification

131 utilisateurs ont participé à l'étape de création des règles du *module de classification*. Ils ont été contactés individuellement à travers Facebook. La collecte des données a duré 2 mois entre Mars et Avril 2011. Ces données représentent un échantillon d'utilisateurs de différents âges et de divers emplacements géographiques. Un utilisateur ne peut participer qu'une fois et les participants qui ne répondent pas complètement au questionnaire posé ont été écartés.

L'ensemble des règles obtenues suite à l'application de l'algorithme *C4.5* est illustré par la figure 27.

Classification Tree	Class
nb_pic <=256.000	3
nb_friends <=102.500	3
age <=27.500	1
nb_friends <=54.500	1
nb_friends >54.500	2
age >27.500	1
nb_friends >102.500	3
nb_publish_week <=10.330	2
nb_pic <=94.000	2
nb_group <=388.500	2
nb_group >388.500	2
sensitive_data = 0	3
sensitive_data = 1	2
nb_pic >94.000	3
nb_friends <=311.000	2
nb_pic <=110.000	3
nb_pic >110.000	2
nb_friends >311.000	3
nb_publish_week >10.330	3
sex = 0	3
age <=22.500	4
nb_publish_week	
<=31.595	
age <=18.500	3
age >18.500	2
nb_publish_week >31.595	4
nb_friends <=281.500	3
nb_friends >281.500	4
age >22.500	3
age <=27.500	3
nb_pic <=63.000	3
nb_pic <=49.500	3
nb_pic >49.500	2
nb_pic >63.000	3
age >27.500	2
sex = 1	3
nb_pic >256.000	4

Figure 27 : L'ensemble des règles extraits de l'arbre de décision

La *matrice de confusion* a été calculée pour déterminer les résultats de prédiction de notre *arbre de décision*, ainsi que l'*accuracy evaluation* pour évaluer la précision des résultats. Ce sont des paramètres couramment utilisés en statistique pour mesurer la qualité d'un système de classification (Bramer 2007).

Les valeurs de la *matrice de confusion* sont présentées au tableau 5. La ligne correspondant au niveau *critique* révèle les prévisions suivantes: 79.3% des profils

*critiques* seront détectés correctement, 13.8% seront considérés comme *très risqué*, 6.94% comme *moyennement risqué* et 0% comme *peu risqué*. Les profils *risqués* seront correctement détectés à 61.7% des fois, les profils *moyennement risqués* à 58.5% des fois et les profils *peu risqués* à 85.7% des fois.

**Tableau 5. Matrice de confusion**

		Classes prédictes			
		Low	Medium	Risky	Critical
Classes actuelles	Low	85.7.0 %	14.3 %	0.0 %	0.0 %
	Medium	7.3 %	58.5 %	31.7 %	2.4 %
	Risky	0.0 %	27.7 %	61.7 %	10.6 %
	Critical	0.0 %	6.9 %	13.8 %	79.3 %

Le tableau de L'*accuracy evaluation* (voir tableau 6) nous permet de dire que l'estimation moyenne du niveau de certitude de la classification lorsque nous l'appliquons à un nouvel échantillon est 67.18%. Il serait intéressant de vérifier la variation de ce pourcentage lorsqu'on considère un grand échantillon d'utilisateurs.

*Sensitivity* et *Specificity* révèlent que notre *module de classification* arrive à identifier les résultats positifs à 85.71% et les résultats négatifs à 97.44%.

Le paramètre *precision* indique que le pourcentage d'obtenir les mêmes résultats dans des conditions inchangées est 80%. Ce qui est un bon résultat en soi.

**Tableau 6. Accuracy evaluation**

	Classification accuracy	Sensitivity	Specificity	Precision
<b>C4.5</b>	0.6718	0.8571	0.9744	0.8000

Le paragraphe suivant présente les résultats de la validation du *module de classification*, du *Filtre à base de connaissance* et du *Filtre communautaire*.

## 6.2 Module de recommandation

163 différents utilisateurs de Facebook ont accepté de participer à la validation de *Protect\_U*. Aucun de ces participants n'avait été sollicité lors de la *classification*. Grâce à un questionnaire, les participants ont pu commenter la pertinence des recommandations affichées ainsi que la précision des *amis de confiance* trouvés. Le questionnaire teste également s'ils sont prêts à changer leurs comportements sur Facebook suite aux recommandations qui leur sont proposées. La figure 28 donne un aperçu de ce questionnaire.

**Merci de répondre à ce questionnaire:**

**1- Combien parmi les personnes dont les images sont affichées ci-haut font partie de vos amis proches?**

Aucune image n'est affichée  
 Aucune personne  
 Certaines personnes  
 La plupart  
 Toutes

**2- Considérez-vous que le niveau de risque affiché s'applique à votre profil?**

Non  
 Oui  
 Je ne sais pas

**3- Pensez-vous que ces recommandations s'appliquent à votre cas et peuvent améliorer la sécurité de votre profil?**

Aucune recommandation n'est affichée  
 Non  
 Oui  
 Je ne sais pas

**4- Êtes-vous prêt à appliquer ces recommandations?**

Aucune recommandation n'est affichée  
 Non  
 Oui  
 Je ne sais pas

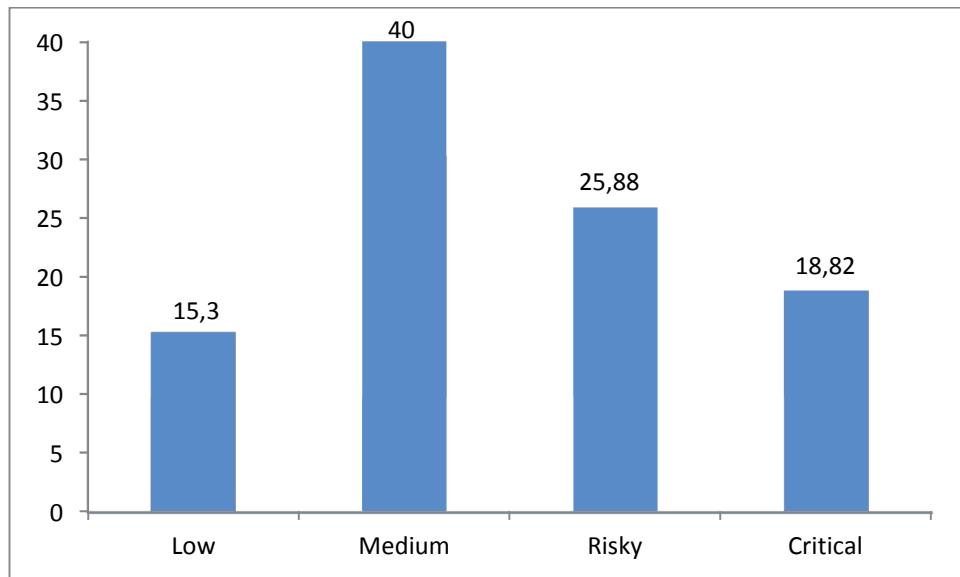
**5- Après l'exécution de cette application, êtes-vous prêt à changer votre comportement et rendre votre profil plus sécuritaire?**

Non  
 Oui  
 Je ne sais pas

**Envoyer**

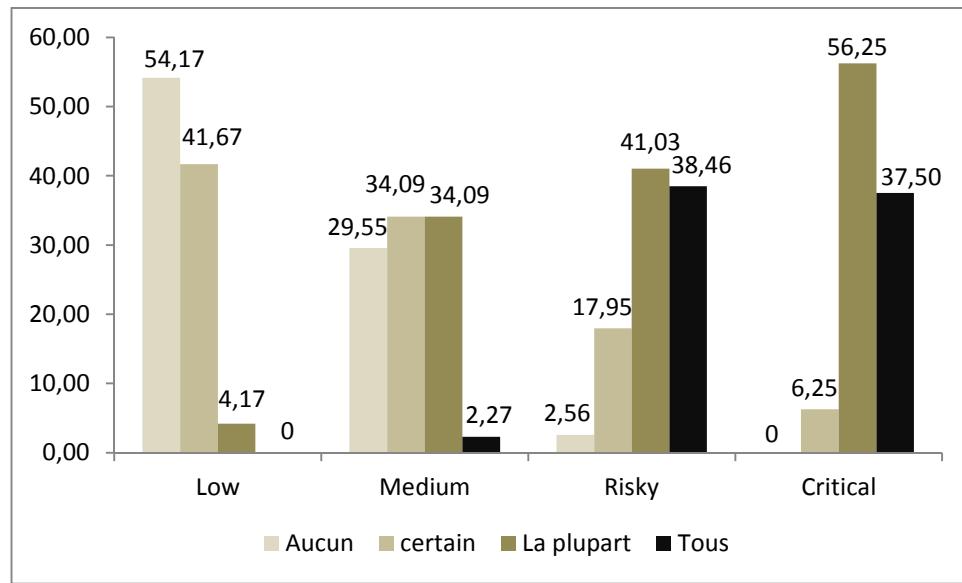
Figure 28. Le Questionnaire de validation

La répartition du *niveau de risque* de ces participants est donnée par la figure 29. 15.30% ont un profil *peu risqué*, 40% ont un profil *moyennement risqué*, 25.88% ont un profil *risqué* et 18.82% ont un profil *critique*.



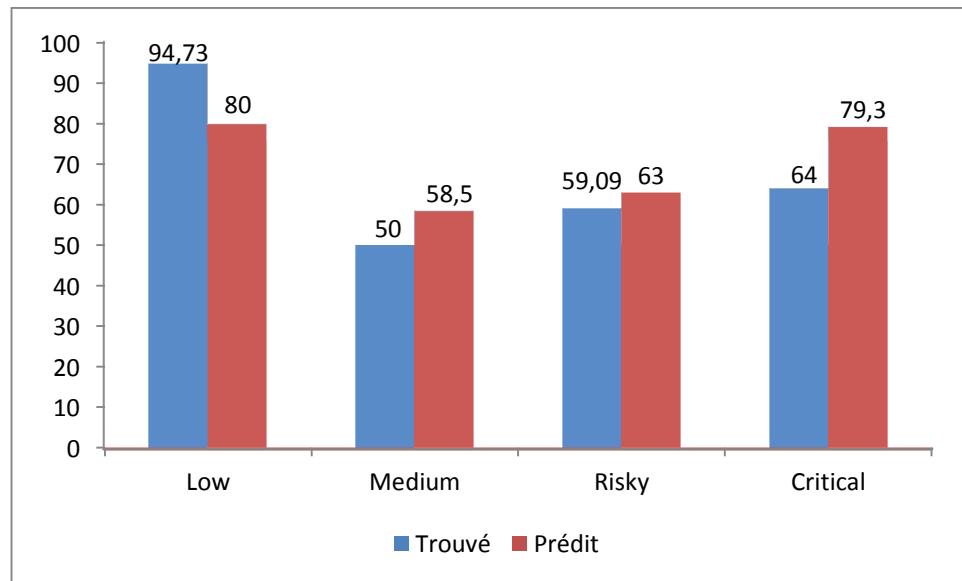
**Figure 29 : Le pourcentage des participants par niveau de risque**

La figure 30 montre que Protect\_U a réussi à reconnaître 79.49% [41.03% + 38.46%] des *amis de confiance* dans le cas de profils risqués et 93.75% [56.25% +37.50%] dans le cas des profils *critiques*. Cependant, pour les utilisateurs à profil *moyennement risqué*, Protect\_U a pu déterminer les *amis de confiance* seulement à 36.36% [34.09%+2.27%]. Le pourcentage chute à 4.17% pour les profils *peu risqués*. Ce dernier résultat n'est pas très surprenant vu que nous affectons aux paramètres *liens de connaissance* (famille et amis proches) et *messages échangés* (formule 2) les plus grandes pondérations. Généralement, les valeurs de ces deux derniers paramètres ne sont pas élevées dans le cas où le profil est *moyennement risqué* ou *peu risqué*. Comme la détection des *amis de confiance* est faible dans ces deux cas, Protect\_U choisit les dix premiers amis qui ont obtenu le poids le plus élevé en appliquant la formule 2, même si parmi eux il y a des amis qui ne sont pas considérés comme étant des *amis de confiance*. Ceci sera utile surtout pour les profils qui sont surclassés par Protect\_U vu que la prédiction de trouver la bonne classe n'est pas parfaite (voir tableau 5).



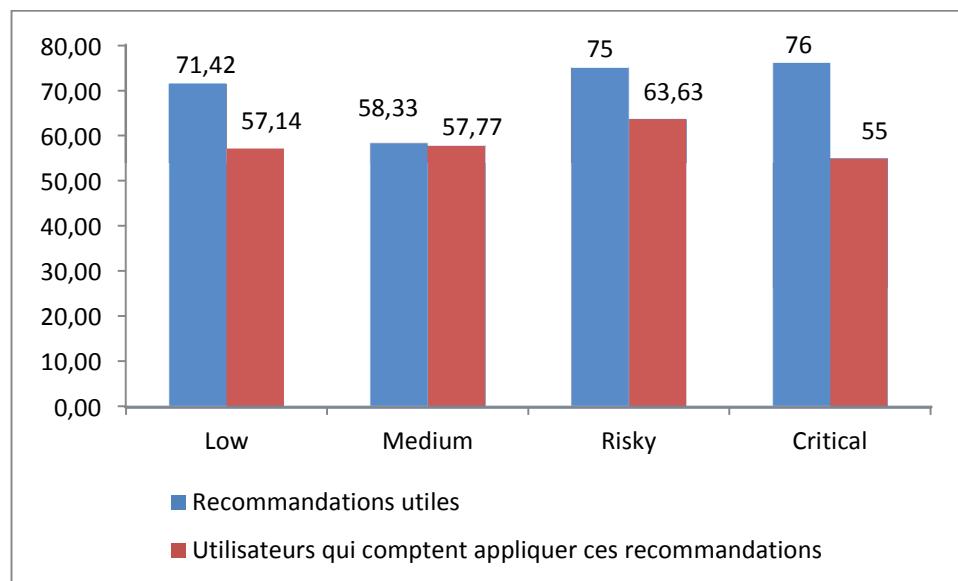
**Figure 30 : Précision de la sélection des amis de confiances par niveau de risque**

La réponse à la question 2 du questionnaire (considérez-vous que le niveau de risque affiché s'applique à votre profil ?), nous ont permis de tirer les résultats de la série « Found » de la figure 31.



**Figure 31 : Profile trouvé vs profile prédict**

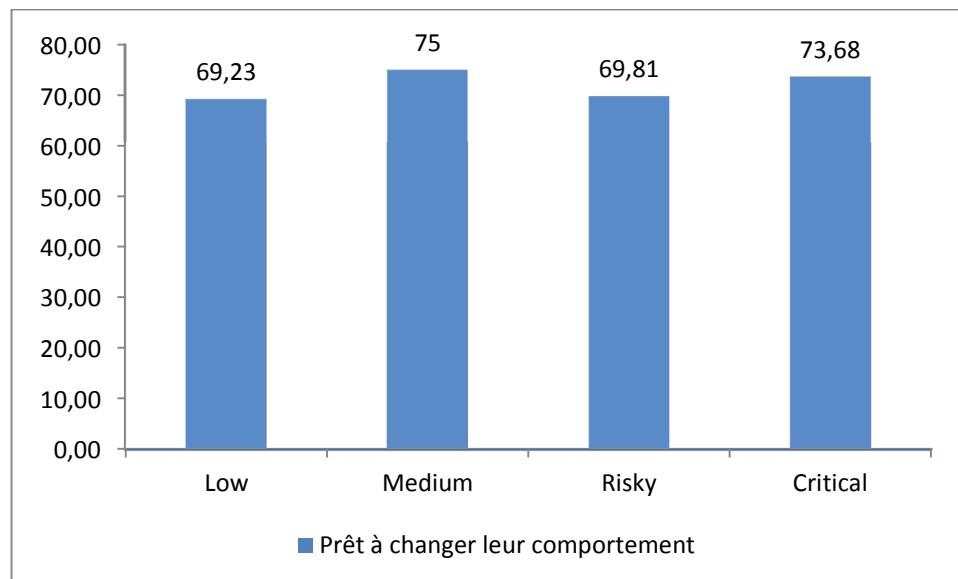
Cette dernière montre clairement que les résultats du profil *peu risqué* dépassent largement les prévisions. En revanche, ceux du profil *critique* n'arrivent pas à atteindre la valeur de la prévision. Ce résultat est relativement facile à comprendre dans la mesure où les utilisateurs étaient contents lorsque leurs profils ont été diagnostiqués à *faible risque* et ils l'ont confirmé sans hésitation. Dans le cas des profils *critiques*, ce ne sont pas tous les participants qui ont apprécié ou accepté que leur profil soit considéré comme *critique*. En revanche, les résultats des profils à *risque moyen* et risqué coïncident relativement bien avec les prévisions.



**Figure 32 : Pourcentage des recommandations jugées utiles par utilisateur, et pourcentage des utilisateurs qui comptent appliquer ces recommandations**

Par ailleurs, plus que 70.18% *en moyenne* des répondants ont trouvé que les recommandations qui leur ont été proposées étaient utiles (voir figure 32). Cependant, uniquement 58.38% *en moyenne* de ces participants étaient prêts à tenir compte des recommandations. Ce résultat est un peu surprenant vu que 71.93% des répondants en moyenne avaient répondu qu'ils étaient prêts à changer leurs comportements (voir figure 33). De plus, ce sont les utilisateurs qui ont un profil *critique* qui étaient les plus réticents à appliquer ces recommandations. Ceci pourra s'expliquer par le fait que dans leur cas le nombre des recommandations à appliquer était élevé et aurait découragé beaucoup d'entre eux à les appliquer.

Un autre groupe réticent à appliquer les recommandations proposées est celui qui contient les profils à *risque faible*. Cette réticence peut s'expliquer par le fait que *Protect\_U* leur a proposé peu de recommandations à respecter, ou bien ils n'ont pas senti l'urgence d'agir vu que leur profil a été classé comme *peu risqué*.



**Figure 33 : Pourcentage des utilisateurs qui sont prêts à changer leur comportement par niveau de risque**

Le questionnaire nous ont permis aussi de constater que 71.93% des participants en moyenne étaient prêts à changer leurs habitudes de comportement sur Facebook suite à l'affichage des recommandations. La figure 33 donne les pourcentages exacts par niveau de risque. Ce résultat laisse à présager que les utilisateurs des réseaux sociaux ne sont pas toujours conscients du danger qu'ils encourrent lorsqu'ils s'exposent des informations sensibles. Cependant certains ont besoin qu'ils soient interpellés directement pour réagir. Un rôle qu'un bon système de protection de vie privée peut et doit jouer.

## Chapitre 7 : Conclusion

Depuis leur apparition, les réseaux sociaux ont vu leur nombre d'utilisateurs augmenter à très grande vitesse pour devenir les sites les plus visités sur internet. Cet engouement est dû à la nature de ces sites qui regroupent d'innombrables fonctionnalités attractives pour les utilisateurs tels que le chat, le partage de photos et la création de nouvelles rencontres.

Plus le nombre d'utilisateurs augmente, plus la quantité d'informations privées partagées par ces sites est conséquente. Ce qui fait apparaître plusieurs problèmes liés à la protection de la vie privée tels que la cyber intimidation, le vol d'identité, le hameçonnage... Tous ces problèmes ont emmené les chercheurs à se poser la question « comment protéger les informations sensibles des utilisateurs des réseaux sociaux ». Plusieurs solutions ont été trouvées pour réduire ce risque que ce soit en proposant des modifications que les utilisateurs peuvent appliquer pour renforcer la protection de leurs comptes, ou bien en assistant les utilisateurs à faire ces modifications de façon automatique.

C'est dans ce contexte que nous avons présenté *Protect\_U*, un système permettant d'améliorer la vie privée des utilisateurs de Facebook. Il est constitué de deux modules: le *module de classification* et le *module de recommandations*. Au niveau du premier module, nous avons consulté 131 participants de Facebook tout en récoltant des paramètres clés de leurs comptes dans le but de créer une base de données. C'est grâce à cette dernière que nous avons pu extraire un ensemble de règles qui nous ont permis de diviser les profils en quatre classes disjointes : *peu risqué*, *moyennement risqué*, *risqué* et *critique*. En fonction des règles trouvées et des classes obtenues, nous avons associé une ou plusieurs recommandations aux utilisateurs afin de leur permettre de réduire le niveau de risque de leurs comptes. Quant au *module de recommandations*, les *règles de classification* ont été appliquées sur 163 nouveaux participants et des recommandations leur ont été suggérées. Suite à ces recommandations, en moyenne 70.18% des

participants les ont trouvées pertinentes et 71.93% étaient prêts à changer leurs comportements. Dans le but de mieux personnaliser les recommandations, nous avons proposé dans ce deuxième module une approche appelée *protection communautaire*. Ceci incite des *amis de confiance* d'un utilisateur donné à participer et à surveiller le contenu de son compte afin de signaler toute anomalie. Pour cela, *Protect\_U* utilise une fonction pour détecter les *amis de confiance* en se basant sur le *lien de connaissance* avec l'utilisateur, *le nombre des messages échangés*, le nombre de fois que l'ami est tagué et le *niveau de risque* du profil de l'ami dans le cas où il a déjà exécuté *Protect\_U*.

Cette fonction arrive à reconnaître les *amis de confiance* dans la majorité des cas, ainsi pour les profils *critiques* nous obtenons 93.75% et pour ceux qui sont *risqués* 79.49%.

Les résultats présentés dans ce travail donnent une idée sur la tendance qu'ont les usagers de Facebook à protéger ou pas leurs vies privées. Pour une expérimentation à grande échelle, il serait possible d'ajuster les paramètres de *Protect\_U* pour qu'il soit exécutable sur la plateforme de développement Open Social qui est utilisée par des réseaux sociaux comme *Google+*, *MySpace2* et *Friendster*.

Il serait également intéressant d'élargir les fonctionnalités de *Protect\_U* pour lui donner la possibilité de protéger l'utilisateur d'amis mal intentionnés en analysant, entre autres, le contenu des images affichées et des textes offensants. Nous pensons dans un futur proche ajouter d'autres modules qui permettraient d'atteindre ce but.

Nous tenons enfin à préciser que nous avons respecté tout au long de notre recherche les aspects éthiques et légaux. Toutes les informations récoltées sur les comptes des participants sont restées anonymes.

Notre travail a été accepté pour publication dans le journal « Journal of Information Security Research ».

## Références

- Adu-Oppong, F., C. K. Gardiner, et al. (2008). Social Circles: Tackling Privacy in Social Networks. The 4th Symposium on Usable Privacy and Security (SOUPS). Pittsburgh, PA, USA.
- Aïmeur, E., G. Brassard, et al. (2008). Experimental Demonstration of a Hybrid Privacy-Preserving Recommender System. ARES: 161-170.
- Aïmeur, E., S. Gambs, et al. (2010). Towards a Privacy-Enhanced Social Networking Site. Availability, Reliability, and Security, 2010. ARES '10 International Conference on.
- Aïmeur, E., S. Gambs, et al. (2010). Towards a Privacy-Enhanced Social Networking Site. Availability, Reliability, and Security, 2010. ARES '10 International Conference on. Krakow, Poland: 172-179.
- Aïmeur, E. and D. Schönfeld (2011). The ultimate invasion of privacy: Identity theft. Privacy, Security and Trust. Montréal, Canada: 24-31.
- Baldazzi, M., C. Platzer, et al. (2010). Abusing social networks for automated user profiling, RAID'2010, 13th International Symposium on Recent Advances in Intrusion Detection, September 15-17, 2010, Ottawa, Canada / Also published in "LNCS", Volume 6307/2010.
- Bilge, L., T. Strufe, et al. (2009). All your contacts are belong to us: automated identity theft attacks on social networks. Proceedings of the 18th international conference on World wide web. Madrid, Spain, ACM: 551-560.
- Bin, Z. and P. Jian (2008). Preserving Privacy in Social Networks Against Neighborhood Attacks. Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on.
- Bonneau, J., J. Bonneau, et al. (2009). The Privacy Jungle: On the Market for Privacy in Social Networks. WEIS '09: Proceedings of the Eighth Workshop on the Economics of Information Security. London, UK.
- Boyd, D. and N. B. Ellison (2007). "Social Network Sites: Definition, History, and Scholarship." Journal of Computer-Mediated Communication 13(1-2).
- Bramer, M. A. (2007). Principles of Data Mining. London, UK, Springer.
- Brown, G., T. Howe, et al. (2008). Social networks and context-aware spam. Proceedings of the 2008 ACM conference on Computer supported cooperative work. San Diego, CA, USA, ACM: 403-412.
- Canada, S. (2009). General Social Survey - Social Networks (GSS).
- Carmagnola, F., F. Verner, et al. (2009). SoNARS: A Social Networks-Based Algorithm for Social Recommender Systems. Proceedings of the 17th International Conference on User Modeling, Adaptation, and Personalization: formerly UM and AH. Trento, Italy, Springer-Verlag: 223-234.
- Chew, M., D. Balfanz, et al. (2008). (Under)mining Privacy in Social Networks. Proceedings of W2SP 2008: Web 2.0 Security and Privacy. Oakland, CA, USA.
- Coronges, K., R. Dodge, et al. (2012). The Influences of Social Networks on Phishing Vulnerability. System Science (HICSS), 2012 45th Hawaii International Conference on.
- Cushman, D. (2010). Reed's law and how multiple identities make the long tail just that little bit longer. Proceedings of the 2008/2009 international conference on Social software: recent trends and developments in social software. Cork, Ireland, Springer-Verlag: 123-130.

- Danezis, G. (2009). Inferring privacy policies for social networking services. *Proceedings of the 2nd ACM workshop on Security and artificial intelligence*. Chicago, Illinois, USA, ACM: 5-10.
- Fang, L. and K. LeFevre (2010). Privacy wizards for social networking sites. *Proceedings of the 19th international conference on World wide web*. Raleigh, North Carolina, USA, ACM: 351-360.
- Fogel, J. and E. Nehmad (2009). "Internet social network communities: Risk taking, trust, and privacy concerns." *Computers in Human Behavior* **25**(1): 153-160.
- Griffith, V. and M. Jakobsson (2005). Messin' with Texas Deriving Mother's Maiden Names Using Public Records. *ACNS*: 91-103.
- Hélou, C., A. E. Gandouz, et al. (2012). "A Privacy Awareness System for Facebook Users." *Journal of Information Security Research*.
- Hernando, A., D. Villuendas, et al. (2010). "Unravelling the size distribution of social groups with information theory in complex networks." *The European Physical Journal B - Condensed Matter and Complex Systems* **76**(1): 87-97.
- Hong, J. (2012). "The state of phishing attacks." *Commun. ACM* **55**(1): 74-81.
- Hussey, J. (2011). Twitter in higher education from application to alumni relations. *Higher education administration with social media: including application in student affairs, enrollment management, alumni relations, and career centers*. Howard House, Wagon Lane, Bingley BD16 1WA, UK, Emerald Group Publishing Limited: 251.
- Irani, D., S. Webb, et al. (2009). Large Online Social Footprints-An Emerging Threat. *2009 International Conference on Computational Science and Engineering (CSE)*. Vancouver, BC, Canada, IEEE. **3**: 271-276.
- Kantardzic, M. (2011). *Data Mining: Concepts, Models, Methods and Algorithms*. New York, NY, USA, John Wiley & Sons, Inc.
- Korolova, A., R. Motwani, et al. (2008). Link privacy in social networks. *Proceedings of the 17th ACM conference on Information and knowledge management*. Napa Valley, California, USA, ACM: 289-298.
- Lederer, S., I. Hong, et al. (2004). "Personal privacy through understanding and action: five pitfalls for designers." *Personal Ubiquitous Comput.* **8**(6): 440-454.
- Leskovec, J. and E. Horvitz (2008). Planetary-scale views on a large instant-messaging network. *Proceedings of the 17th international conference on World Wide Web*. Beijing, China, ACM: 915-924.
- Lipford, H. R., A. Besmer, et al. (2008). Understanding privacy settings in facebook with an audience view. *Proceedings of the 1st Conference on Usability, Psychology, and Security*. San Francisco, California, USENIX Association: 1-8.
- Liu, K. and E. Terzi (2010). "A Framework for Computing the Privacy Scores of Users in Online Social Networks." *ACM Trans. Knowl. Discov. Data* **5**(1): 1-30.
- Ma, H., D. Zhou, et al. (2011). Recommender systems with social regularization. *Proceedings of the fourth ACM international conference on Web search and data mining*. Hong Kong, China, ACM: 287-296.
- Maximilien, M. E., T. Grandison, et al. (2009). Privacy-as-a-Service: Models, Algorithms, and Results on the Facebook Platform. *Proceedings of W2SP 2009: Web 2.0 Security and Privacy*. Oakland, CA, USA.
- Mazzia, A. L. K. and E. Adar (2011). The pviz comprehension tool for social network privacy settings. *UMTech Report*.

- Narayanan, A. and V. Shmatikov (2009). De-anonymizing social networks. 2009 30th IEEE Symposium on Security and Privacy: 173-187.
- Ninggal, M. and J. Abawajy (2011). Privacy Threat Analysis of Social Network Data, Algorithms and Architectures for Parallel Processing. Y. Xiang, A. Cuzzocrea, M. Hobbs and W. Zhou, Springer Berlin / Heidelberg. **7017**: 165-174.
- Patil, S. and A. Kobsa (2010). "Enhancing privacy management support in instant messaging." Interact. Comput. **22**(3): 206-217.
- Power, R. (2011). Child Identity Theft.
- Reeder, R. W., L. Bauer, et al. (2008). Expandable grids for visualizing and authoring computer security policies. Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems. Florence, Italy, ACM: 1473-1482.
- Ryan, N., P.-E. Lavoie, et al. (2011). Note de recherche no. 13. La fraude via les médias sociaux, Syngress.
- Soman, K. P., S. Diwakar, et al. (2006). Insight into Data Mining: Theory and Practice, Prentice-Hall of India Pvt.Ltd.
- Stone-Gross, B., T. Holz, et al. (2011). The underground economy of spam: a botmaster's perspective of coordinating large-scale spam campaigns. Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats. Boston, MA, USENIX Association: 4-4.
- Timm, C. and R. Perez (2010). Seven Deadliest Social Network Attacks, Syngress.
- Up2social (2011). Le social et l'avenir de la communications. <http://up2social.com/livre-blanc-social-avenir-communication/>.
- Yan, J. and A. S. E. Ahmad (2008). A low-cost attack on a Microsoft captcha. Proceedings of the 15th ACM conference on Computer and communications security. Alexandria, Virginia, USA, ACM: 543-554.
- Zheleva, E. and L. Getoor (2009). To Join or not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles. 18th International World Wide Web conference (WWW).