FACEBOOK, DANGER !

GUI_G

–

http://www.facebook-danger.org | www.guig.fr

–

17 MAI 2009

VERSION CORRIGEE (V1.0)

PREAMBULE :

- Pourquoi avoir fait cet article ?

Au fil du temps, en consultant différents sites et blogs et en parlant avec certains amis, je me suis rendu compte que Facebook pouvait être détourné de son idée d'origine dans le but de collecter les données personnelles des utilisateurs. J'ai aussi fait le constat accablant que beaucoup d'internautes ne prennent pas garde aux informations qu'ils transmettent, les plus jeunes en particulier. La majorité ne se rend pas compte des risques qu'ils encourent à diffuser sans réflexion secrets, commentaires salaces, vidéos chocs, dans un monde virtuel où les échanges d'informations sont plus massifs de jour en jour et où les règlementations en vigueur ne sont pas encore claires et différent d'un pays à l'autre. Ainsi, je suis convaincu de la nécessité de ce document pour avertir les utilisateurs de réseaux sociaux et leur permettre de se protéger.

- Que risque-t-on ?

Plus qu'on ne le croit. Tout d'abord, il faut voir les informations que l'on risque de divulguer, c'est-à-dire celles qu'on met en ligne : beaucoup d'informations sur nous-mêmes et nos amis, notre vie, tout simplement. Ce document est fait dans le but de montrer les dangers, les risques du site de réseautage social Facebook (et les autres, par extension).

- À qui s'adresse ce document ?

À tout le monde, aux utilisateurs de Facebook et des réseaux sociaux en premier lieu, mais aussi à tous les autres internautes en général.

J'essaierai d'être le plus clair possible afin d'être lu et compris par tout le monde. Si toutefois vous avez des doutes, des questions ou remarques, vous pouvez aller sur le site dédié à cet article : http://www.facebook-danger.org. Si vous ne trouvez pas ce que vous voulez, vous pouvez nous joindre à cette adresse : facebook.danger@gmail.com. Vous pouvez aussi me retrouver sur mon blog à cette adresse : http://www.guig.fr.

Afin de rester dans ce contexte du Web 2.0, je suis aussi joignable par Twitter et sur Facebook !

SOMMAIRE :

INTRODUCTION :

Facebook, tout le monde en parle : dans la rue ou le métro, dans les journaux ou à la télé, entre amis ou entre collègues bref ; partout. On entend vaguement parler des risques liés à Facebook: respect de la vie privée, virus, pédophilie… Facebook est une mine d'informations décrivant un portrait complet de ses utilisateurs, et beaucoup de personnes s'intéressent à ces précieuses données.

Et les utilisateurs dans tout ça ? Quels sont les vrais problèmes de vie privée avec Facebook? Que mettons-nous en jeu en s'y inscrivant? On essayera ici de référencer de manière complète les différents problèmes de sécurité susceptibles d'être rencontrés sur Facebook autant sur le plan viral que sur la protection des données personnelles. Je tiens à prévenir que je ne m'intéresserais au succès de Facebook et aux d'un tel que pour expliquer les différents problèmes qu'ils entraînent.

Nous commencerons par une rapide présentation du réseau social. Nous étudierons ensuite les dangers de Facebook en commençant par aborder les risques viraux, puis les dangers concernant la vie privée des internautes. Enfin, nous terminerons en récapitulant les risques et en proposant un regard critique sur l'avenir de Facebook et des services du Web 2.0 en général.

PRESENTATION : FACEBOOK, KESAKO?

Facebook est un « réseau social » créé en 2004 dans la très célèbre université américaine *Harvard* par un de ses étudiants, Mark Zuckerberg. Le but premier du réseau était d'agir comme un trombinoscope (*facebook* en anglais) afin que les filles et les garçons de l'école puissent se rencontrer plus facilement. Le réseau se développa rapidement, d'abord à d'autres universités puis apparut une version publique, multilingue et mondiale. En décembre 2009, le réseau social compte aujourd'hui 350 millions d'adeptes, ce chiffre est en constante évolution et cela ne semble pas prêt de s'arrêter comme nous le montrent les évolutions positives du chiffre d'inscrits (jusqu'à 37% par semaine dans certains pays).

Un *réseau social* à pour vocation première de rassembler les gens grâce à internet. Des amis perdus, de la famille éloignée ou des collègues et même des inconnus, Facebook vous met en relation avec le monde entier peu importe qui, peu importe quand, peu importe où. Mais aujourd'hui le rôle d'un *site de réseautage* ne s'arrête pas là : vous pouvez par exemple échanger des vidéos ou des photos avec vos amis, jouer avec eux en ligne, ou bien vous amuser avec des petites applications directement disponibles sur le site. A l'heure actuelle, les principaux réseaux sociaux sont : Facebook (le plus important, qui creuse l'écart), MySpace (orienté art : musique essentiellement), Twitter, (service de *micro-blogging* : l'utilisateur publie des phrases de 140 caractères maximum), Flickr (partage de photos), LinkedIn (réseau professionnel) ou encore, au niveau Français, Copains d'avant (cursus scolaire). Il en existe encore d'autres, orientés vers d'autres aspects (par exemple sur les goûts : Ulike) mais je vous cite ici les plus importants en termes d'inscrits et les plus connus.

Le succès de Facebook est aujourd'hui évident ; en quelques chiffres, nous avons : 350 millions d'utilisateurs ; un capital auto-estimé à 8 milliards de dollars après seulement 5 ans de vie, 250 000 nouveaux membres par jour, environ 10% de la population française, capte près de 29,5% du flux total sur internet, 80 milliards de photos chargés sur le site, 63,9% des internautes français ont déjà visité un site de réseautage selon une récente étude de *Comscore*, ce pourcentage montant à 74,6% pour la population européenne. Facebook dépasse même SkyRock, reconnu pour sa popularité chez les jeunes. Son public, même s'il s'étend aux autres générations, est le plus gourmand d'Internet et des nouvelles technologies : les 18-24 ans. Les adolescents sont d'ailleurs les nouvelles cibles (et ce sont les plus crédules) : partageant leur vie pendant 1h40 par semaine sur Facebook selon une estimation *CyberSentinel.co.uk.* Ces chiffres donnent le vertige, et nous montrent que Facebook est aujourd'hui

plus puissant que jamais.

I] LES MENACES VIRALES :

1) UN SITE COMME TOUS LES AUTRES

Facebook à peut être un nombre considérable de visiteurs par jour et d'inscrits sur son site, il n'en demeure pas moins vulnérable. Il est important de savoir que même si les ingénieurs, développeurs et testeurs employés par Facebook travaillent d'arrache-pied jour et nuit pour en faire le service le plus fiable et le plus sécurisé au monde, le site sera toujours vulnérable. « Facebook, tous comme les autres systèmes informatiques n'est pas à l'abri d'une attaque, d'une faille » nous dit Damien BANCAL, journaliste et fondateur du site www.zataz.com, spécialisé en cybercriminalité. Il y a déjà eu plusieurs précédents (cf. Sources). La Politique de confidentialité (que j'abrègerai P.C.) de Facebook nous rappelle par ailleurs qu' « Il n'existe aucun système de sécurité infaillible. ». Félix Aimé, passionné d'informatique, ajoute que « tout système informatique est vulnérable ». De plus, Facebook à un succès très important, à travers le monde entier et sa richesse, qui est sa principale qualité, est aussi son principal défaut : c'est cette richesse qui va pousser certains pirates à tenter de détourner et d'attaquer le réseau et ses utilisateurs.

2) LES FAILLES XSS

Les failles XSS (*Cross Site Scripting*) se basent sur les vulnérabilités d'un site, c'est-à-dire une erreur dans le code source (le code source est un peu comme une « recette ») du site. Lorsqu'un utilisateur peut rentrer des informations dans un champ, une protection doit être mise en place afin qu'un pirate ne puisse pas rentrer un code malicieux, qui pourrait détourner le site en volant, par exemple, les cookies et les sessions des utilisateurs. Ce genre de failles est assez peu répandu sur le site, mais il y a eu des précédents comme en décembre 2008 ou en février dernier.

3) KOOBFACE, LE VIRUS QUI MET FACEBOOK A L'ENVERS

Koobface est un virus dans le sens où c'est un programme malveillant mais on peut le considérer plus particulièrement comme ver, c'est-à-dire, selon Wikipédia, « un logiciel malveillant qui se reproduit sur des ordinateurs à l'aide d'un réseau informatique, sans avoir besoin d'un programme hôte pour pouvoir se reproduire ».

Aujourd'hui, le seul virus connu sur Facebook se nomme « Koobface », il s'est principalement répandu en août 2007, et même s'il n'a touché « *qu'un très faible pourcentage d'utilisateurs* » selon Barry Schnitt, porte-parole de Facebook, le virus s'est révélé nuisible pour les utilisateurs affectés : une « simple » collecte d'informations récupérant le nom d'utilisateur, le mot de passe, l'adresse mail, les codes de cartes bancaires…

Koobface a un fonctionnement « typique » et déjà connu : il se sert de la naïveté des internautes pour évoluer et se répandre. Voici les différentes étapes d'une contamination :

On nommera Victime 1 et Victime 2 les deux personnages de cet exemple.

1. Victime 1 reçoit de son ami Victime 2 un message sur Facebook, où est écrit « Tu es trop beau sur cette vidéo » ou un simple « LOL » afin d'attiser la curiosité de Victime 1 et l'amener à cliquer sur le lien.

2. Victime 1 clique sur le lien l'amenant vers une vidéo sur laquelle il s'attend à se voir ou à rire. Cependant, en arrivant sur la page (qui est une fausse page avec une fausse vidéo) un message lui demande d'installer la dernière version de *Flash Player* (permettant, entre autres, d'utiliser les services de streaming audio et vidéo) pour pouvoir lire la vidéo.

3. Victime 1 télécharge le fichier d'installation frauduleux et l'installe sur son ordinateur. A partir de cela, Victime 1 est infecté et va répandre à son tour le virus contre son gré. Le ver, après son installation, se sert ensuite de l'ordinateur vérolé pour se répandre, il envoie à travers le compte Facebook de la victime ainsi que son compte *MySpace* le même message que celui reçu précédemment. Le virus peut donc se répandre à une vitesse impressionnante simplement grâce à la naïveté de l'utilisateur.

Mais les créateurs de virus ne s'arrêtent pas à ce point là. En effet, après quelques semaines, le virus Koobface voyait déjà de nouvelles versions, provoquant une nouvelle vague de virus. On estime aujourd'hui à 20 000 le nombre de ces « cousins » de Koobface. Nous verrons dans la troisième partie comment se prémunir contre ce type d'attaque.

4) DU FAUX PARTOUT

Après les liens vers les fausses vidéos et les feux Flash Player, il existe aussi les « faux Facebook ». Ces sites reprennent le design du site de Facebook et tentent de faire croire à l'internaute qu'il est bien sur le site qu'il prétend. La similitude est frappante et il est très difficile de trouver une différence dans le design du site. L'internaute qui se rend sur cette page rentre son identifiant et son mot de passe puis est redirigé vers le véritable site de Facebook. Sans le savoir, l'internaute vient de donner toutes ces informations à un pirate. Il donne même son compte : le pirate peut le reprendre et publier des éléments qui pourraient ternir la réputation de la victime.

Pareillement, des attaques par *phishing* (ou *hameçonnage*) ont eu lieu sur Facebook. Encore une fois, le principe de ce genre d'attaque est très simple. Un utilisateur reçoit un mail qu'il croit être d'un service de Facebook mais provenant d'un pirate. Ce mail l'invite à se connecter sur le site de Facebook en lui proposant directement le lien. L'internaute clique sur le lien, se retrouve sur une page qui est apparemment celle de Facebook et rentre ces identifiants. Le pirate récupère ainsi l'identifiant et le mot de passe de l'internaute et donc son compte tout entier. Les failles par phishing sont très répandues sur internet, et plus particulièrement sur des sites importants, là où l'impact de l'attaque sera le plus important. eBay et Paypal sont deux sites fréquemment touchés par ce genre d'attaque, leurs dimensions commerciales intéressent en effet particulièrement les pirates.

Il existe également des fausses applications. La plus connue se nomme *The Error Check System.* Elle prévient les utilisateurs d'un problème sur leur profil lors de son visionnage par un contact. En cliquant sur le message, l'internaute installe l'application qui va collecter des informations personnelles sur la victime.

Finalement, nous remarquons que l'on peut trouver sur Facebook beaucoup de fausses informations : faux-comptes, fausses vidéos, fausses applications et même des faux Facebook ! La prudence est donc nécessaire pour ne pas être touché par les différentes menaces. Nous verrons dans la troisième partie comment éviter ce genre d'attaques.

Ainsi, malgré le mal que se donnent les développeurs, Facebook demeure et demeurera un site faillible, comme tous les systèmes informatiques. Certaines attaques se sont révélées très virulentes par le passé, et vu la croissance du réseau social, nous pouvons nous attendre à une augmentation en nombre et en puissance de ces attaques dans l'avenir promettant des jours difficiles aux internautes non-avertis. Nous verrons cela de façon plus approfondie dans la partie intitulée « Les dangers pour la vie privée ».

II] LES DANGERS POUR LA VIE PRIVEE :

1) LES INFORMATIONS FOURNIES PAR L'UTILISATEUR

Tout d'abord, il est important de savoir ce que l'on donne à Facebook. Je dis *à Facebook*, mais une distinction doit être faite : les applications qui sont présentes sur Facebook n'appartiennent pas à Facebook. Nous avons donc un double risque. Lors de notre inscription à Facebook, nous devons donner obligatoirement notre prénom, notre nom, notre adresse mail, notre mot de passe, notre sexe et notre date de naissance. Jusqu'ici, rien de particulier et pourtant une erreur humaine et trop répandue est déjà possible : il ne faut pas oublier qu'une grande partie des internautes utilise le même mot de passe voire le même pseudonyme associé entre les différents services qu'il utilise sur internet. Il suffit dans ce cas là qu'un seul site se voit piraté et l'internaute aura « donné » son mot de passe pour plusieurs sites, adresses mails, ou pire, sites de web-marchands. De cette manière, Damien BANCAL nous confirme que « le plus gros danger reste l'utilisateur lui-même ».

Dès la fin de l'inscription, on nous demande directement d'« afficher et modifier » notre profil. Et là, rien ne va plus ! Les informations demandées sont déjà très précises et nombreuses qui plus est, histoire d'avoir un portrait intégral de l'utilisateur : ville natale, quartier d'origine, situation amoureuse, orientation sexuelle, et même opinion politique et religion. Et encore, nous ne sommes qu'au premier onglet, appelé « Informations générales ». Juste après, nous avons « Informations Personnelles » puis « Coordonnées » et enfin « Formation et Emploi ». Autant dire que Facebook, à travers ce questionnaire connaît les moindres détails de notre personnalité : nos centres d'intérêts et loisir, notre parcours professionnel, notre (nos) numéro(s) de téléphone, il en sait peut-être même plus que notre mère ou que la police ! Et encore, ce n'est toujours pas fini, lors de notre parcours sur Facebook, nous sommes amenés ou encore par des propositions d'amis, soit par une recherche personnelle ou soit par une proposition de Facebook, à devenir « Fan » de quelque chose, ami, avec d'autres personnes suggérées « que l'on peut connaître », ou de devenir membre d'un groupe ; ou bien encore, par des interactions avec les autres utilisateurs à recevoir ou écrire des messages sur *le mur* d'un autre utilisateur (le mur est un espace où les amis de l'utilisateur concerné peuvent laisser des messages. Ce genre de jeux amuse grâce à leur esprit ludique et convivial : l'utilisateur se sent en confiance et croit pouvoir se confier librement. Cette collection de données est interdite par la loi française, mais autorisée par la loi américaine.

2) LES APPLICATIONS PRESENTES SUR FACEBOOK

Des petites applications sont disponibles sur le site de Facebook. Pour la plupart, elles ont une dimension distrayante, n'ayant aucun autre intérêt que d'amuser les internautes. Ces applications permettent d'interagir encore une fois avec l'ensemble de son réseau. Aussi n'est-il pas surprenant de voir le succès de ces applications en plein expansion dans le réseau social, comme le désormais célèbre *Paf le Chien* qui a atteint un million d'utilisateurs une semaine après son lancement. La dimension distrayante attire les utilisateurs, qui pour la plupart n'y voient qu'un moyen de passer le temps agréablement et rapidement, sans prendre conscience de la taille de la porte d'entrée qu'ils laissent derrière eux.

Les applications présentes sur Facebook sont dites des *Black Box.* « Une Black Box est tout simplement une boîte noire où rentrent des informations qui sont traitées à l'intérieur. Nous avons le

résultat de ces dernières à la fin du traitement (à leur sortie) mais nous ne savons pas quel algorithme a réalisé le résultat » nous définit Félix Aimé. Ces applications sont bien des Black Box, « on ne sait pas ce qu'il y a derrière » confirme Félix. De plus, cette montagne d'applications est pour la plupart créée par des amateurs, et qui n'hébergent pas leurs applications sur le serveur de Facebook. Cela peut poser un grave problème de protection des données si le serveur qui héberge l'application est compromis ou si le code de l'application même est mal protégé. « Le tout est d'aujourd'hui savoir où vont aller nos informations personnelles dans le futur... car nous n'avons aucune garantie qu'elles ne soient utilisées par de futures filiales de Facebook (orientées marketing) » poursuit Félix. En clair, cela signifie que les informations fournies à ces services et récupérées par ceux-ci (via une autorisation préalablement acceptée par l'utilisateur) peuvent être récupérées, réutilisées, modifiées sans demander d'autorisation à l'utilisateur.

Même si certaines lois limitent ce genre de cas, il est difficile d'empêcher les abus. Alex TÜRK, sur Ecran.fr le 19 février 2009 se dit « inquiet, affolé même ». La plupart du temps, ces applications ne font « que » récupérer les données déjà présentes sur votre profil. Il est cependant possible que celles-ci fixent des règles particulières. Il est donc nécessaire de prendre en considération l'étendue de l'accès qu'aura l'application lorsque l'on en accepte une. Dans la P.C., Facebook nous explique qu' « avant d'autoriser un développeur de la plate-forme à rendre une application de la plate-forme disponible pour vous, Facebook demande au développeur de la plate-forme d'accepter un accord qui exige notamment le respect de vos paramètres de confidentialité.». Cependant, aucune vérification n'est possible, et les engagements faits par le développeur ne sont pas véritablement contrôlables. Il est d'ailleurs ajouté plus loin « bien que nous ayons pris des dispositions contractuelles et techniques pour réduire le risque d'une mauvaise utilisation de ces informations par les développeurs de la plate-forme, nous ne pouvons pas garantir que tous les développeurs de la plate-forme respecteront ces accords. ». Ainsi, Facebook ne peut pas grand-chose pour protéger les utilisateurs se servant des ces applications, abandonnant sans contrôle une quantité considérable d'informations sur ces utilisateurs. Donc « Facebook ne suit pas ni n'approuve les développeurs de la plate-forme et, par conséquent, ne peut pas contrôler leurs pratiques »… C'est même directement et clairement écrit dans la politique de confidentialité.

3) LE ROLE DE FACEBOOK

Après la polémique de février 2009 causé par le changement des Conditions Générales d'Utilisation (CGU), la vigilance s'impose. Pour rappel, Facebook devenait propriétaire de toutes les informations publiées sur son site et pouvait à tout moment les récupérer, les modifier, les redistribuer ou les revendre. Depuis, Facebook à rebroussé chemin face au mécontentement des internautes et de certaines associations de consommateurs comme l'Electronic Privacy Information Center (EPIC) américaine.

Facebook, d'après sa P.C., veille « à ce que vos données personnelles restent confidentielles » ; « ouf » pourrions-nous soupirer en lisant ceci. Quelque chose tout de même étrange dans cette Politique de Confidentialité (que je vous recommande de lire) : on peut lire beaucoup de choses sur les droits que l'internaute donne à Facebook mais finalement très peu à propos des devoirs de Facebook. On peut y lire deux choses vraiment intéressantes : la première, déjà énoncée plus haut, est que Facebook « veille à ce que nos données restent confidentielles ». Le terme veiller ne rassure pas. La deuxième est vis-à-vis de la publicité présente sur le site : les annonceurs ne possèderaient que *l'adresse IP* du visiteur (une sorte de signature numérique de l'internaute) et pourraient récupérer des

cookies (fichiers temporaires permettant aux sites visités de reconnaitre l'internaute et de voir son activité). Cela paraît très peu, mais grâce à ces informations ont peu déjà géolocaliser l'internaute.

On ne peut pas être très rassuré vis-à-vis de Facebook et de la protection de nos données personnelles, d'une part par la présence trop peu fréquente de garanties et par la fébrilité de ces dernières. Il ne faut pas s'attendre à des miracles de la part de Facebook, même après avoir décidé de faire marche arrière sur les CGU de février dernier. En effet, les informations que l'on donne chaque jour à Facebook lui servent à vivre. « Les données personnelles sont la matière première de Facebook » confirme Jérôme Bouteiller »

4) LE ROLE DE L'UTILISATEUR

Si je décide de finir par le rôle de l'utilisateur, c'est bien parce que celui-ci à la place la plus importante dans l'histoire : c'est lui qui donne ses informations au final. Et c'est à lui de s'autocensurer pour ne pas avoir à le regretter plus tard. Comme nous le confirme Jérôme Bouteiller, co-auteur de *Bienvenue sur Facebook : LE mode d'emploi*, ce sont « les jeunes générations [qui] ont [le] moins d'appréhension à se dévoiler sur le net ». Ces idées sont par ailleurs reprises dans la P.C. de Facebook : « C'est vous qui décidez d'afficher ou non des informations dans votre profil, notamment vos coordonnées et vos informations personnelles, vos photos, vos centres d'intérêt et les groupes dont vous faites partie ».

Même si l'utilisateur est le client et a quelques garanties de la part de Facebook (comme vu plus haut), c'est à lui que revient le rôle le plus important : celui d'être vigilant. Car c'est bien lui-même la source principale de la divulgation de ces données personnelles. Nous verrons dans la troisième partie comment limiter les risques dus à l'utilisation de Facebook. N'oublions pas que ce « que vous publiez sur ce Site Web des informations à vos risques et périls ».

Bien que Facebook explique dans sa Politique de Confidentialité que les données de ses utilisateurs doivent restées confidentielles, il participe au Marketing ciblé, c'est-à-dire que les pubs présentes sur le site sont ciblées selon les goûts identifiés des utilisateurs. Sur ce point là, relativisons : les régies publicitaires ne recevront « que » l'adresse IP et quelques cookies.

Facebook est elle-même une Blackbox, nous ne savons pas où vont réellement nos informations et de jour en jour cette crainte se confirme : les dernières CGU (Conditions Générales d'Utilisation) stipulaient que chaque données laissées sur le réseau par un internaute appartenaient à vie à Facebook.

Malgré quelques garanties présentes dans les Conditions d'Utilisation et la Politique de Confidentialité, il est important de rester vigilant. Face à ces risques, je conseille, tout comme Alex TÜRK, président de la Commission Nationale de l'Informatique et des Libertés (CNIL), la vigilance. Les utilisateurs les plus destinés à avoir des problèmes de vie privée seraient les lycéens et les étudiants : « Nous avons noté que les jeunes générations ont moins d'appréhension à se dévoiler sur le net. Etats d'âme, commentaires salaces, photos ou vidéos déshabillées, les lycéens ou les étudiants vont parfois très loin sur les plates-formes de publication et s'en mordent les doigts quand leurs parents ou leurs employeurs tombent dessus » nous dit Jérôme BOUTEILLER. Les plus jeunes, plus à l'aise avec les nouvelles technologies mais aussi plus enclins à en perdre le contrôle.

III] SE PROTEGER – QUELQUES ASTUCES :

Voici dix petites astuces faites pour vous éviter de partager vos données les plus personnelles avec le monde entier :

1. La désinscription pure et simple. C'est la solution la plus radicale, et, en soit, ce n'en est pas vraiment une. Car, Facebook, aussi dangereux soit-il pour nos données personnelles, est un outil formidable pour partager, parler, s'amuser, apprendre et rencontrer d'autres personnes (et bien plus !). À mon avis, il suffit donc de prendre de bonnes habitudes pour limiter les risques tout en profitant de l'ensemble des avantages qu'il nous offre. Un formulaire de désinscription est disponible à cette adresse : http://www.facebook.com/help/contact.php?show_form=delete_account. Sachez que vos données, même après désinscription, restent sur les serveurs de Facebook : « Si quelqu'un souhaite supprimer sa page Facebook, il faut qu'il sache que l'on ne peut garantir d'y parvenir. » à dit Alex TÜRK dans Metro le 19 avril dernier. Il poursuit « Je dis aux internautes d'être vigilants à propos des informations qu'ils mettent en ligne. ».

2. Accepter ses « vrais amis ». En effet, lors d'une demande d'amis, on a souvent la mauvaise habitude d'accepter sans vraiment réfléchir les personnes qui souhaitent devenir nos amis. Faites donc bien attention d'accepter seulement les personnes que vous connaissez ! N'oubliez pas qu'une personne que vous avez acceptée comme ami aura de vous toutes les informations mises en ligne : photos, coordonnées, messages…

3. Un geste simple, vérifier que l'ami qui vous invite est bien celui que vous pensez : une personne mal intentionnée pourrait se faire passer pour un ami à vous. Vous éviterez ainsi les *faux profils*. Pour vérifier que la personne est bien celle que vous croyez, un simple coup de fil ou un petit mail suffit ! C'est tout simple, et ça évite de nombreux risques.

4. Triez vos amis ! Trier ses amis est une autre solution qui va vous permettre de diffuser ce que vous voulez à qui vous voulez. La première étape est de créer ses listes d'amis et d'y ajouter ses amis dans différents groupes. Il faut aller dans l'onglet « Amis » en haut du site et de créer la liste sur la gauche puis aller dans « Paramètres » (en haut) et choisir « Confidentialité », vous pourrez alors modifier les droits des différents groupes.

5. Ne mettez pas en ligne ce que vous ne voulez pas que l'on sache. Si vous ne voulez pas dévoiler à vos amis votre numéro de téléphone ou votre situation amoureuse, ne le dites pas ! Nos amis peuvent le faire, mais nous ne sommes pas obligés de donner toutes nos informations pour profiter de Facebook.

6. Limitez les accès. Ce point s'inscrit dans la continuité du point 4 qui nous a permis de faire un « tri » des amis. En cherchant dans « Paramètres », vous devriez voir plusieurs options qui vous permettront de choisir qui aura accès à quoi. Entre autres : profil, photos, informations générales, informations personnelles… Choisissez qui aura accès à quoi.

7. Faites attention aux applications. Certaines applications sont très douteuses. Un petit exemple : l'application « Que pensent mes amis de moi ? » ou bien « Have sex » sont à éviter. Ces applications

posent des questions très personnelles et récoltent une mine d'informations sur vous et vos amis. Ces informations pourraient être vendues ou données demain à n'importe qui. De plus, en acceptant les applications, vous acceptez qu'elles aient accès à toutes vos informations. Pour modifier les droits, rendez-vous à « Paramètres » puis « Applications ».

8. Détaguez-vous. Lorsqu'un ami à vous poste une photo sur Facebook et vous tague, c'est-à-dire qu'il marque votre présence sur la photo, cette photo vient directement dans les vôtres ! Ainsi, tout le monde peut les voir, sans que l'ami qui ait posté les photos soit commun. En consultant ladite photo vous cliquer sur « Supprimer le marquage » plus bas.

9. Supprimer son profil public. En allant dans les paramètres de confidentialité, décochez la case « Créer un profil public ». Cela aura pour effet de vous désindexer de Google. Ainsi, une recherche via Google à partir de votre nom et prénom sera impossible.

10. Limitez les informations sur votre mur. Toujours en allant dans l'onglet « Paramètres » puis « Confidentialité » et « Actualités et mur ». Décochez les cases des éléments que vous ne souhaitez pas faire apparaître sur votre mur et de ce fait, sur la page d'accueil de tous vos amis depuis la mise à jour de l'affichage du réseau

Finalement, je vous conseillerai de rester vigilant, en règle générale. Internet et les services du Web 2.0 sont entrés dans les mœurs des Français, et désormais, plus personne ne s'imagine vivre sans. Ils apportent de nombreux avantages à l'internaute, mais il ne faut pas oublier que les informations laissées par celui-ci sont une aubaine pour les pirates, les régies publicitaires et les réseaux eux-mêmes qui ont besoin de financer les services qu'ils offrent. Vos informations sont précieuses et tous les moyens sont bons pour les obtenir. Facebook pourrait devenir le nouveau *Big Brother* constituant une base de données plus grande que n'importe quel gouvernement ou service de police. Ainsi, demandez-vous à chaque fois où vont les informations que vous fournissez, qui peut les avoir, où peuvent-elles ensuite aller ? C'est en se posant ce genre de questions que l'on évolue et que l'on diminue les risques. Internet a de la mémoire et vos informations ne se perdent pas, et si en psychanalyse on peut entendre que « les souvenirs oubliés ne sont jamais perdus » (Sigmund Freud), c'est pourtant au travers d'internet que cette idée se manifeste particulièrement. Peu importe le nombre d'années écoulées, il sera toujours possible qu'une information personnelle soit présente sur la toile. Essayez aussi de varier vos mots de passe, en faisant en sorte que ceux-ci soient longs et complexe : c'est-à-dire : qui ne contient pas de mots présents dans le dictionnaire, avec des chiffres, des lettres majuscules et minuscules, des caractères spéciaux… Une bonne phrase avec des fautes d'orthographes à faire pâlir un professeur de français et un « langage sms » peut faire l'affaire ! Une autre règle s'impose en informatique, peu importe l'utilisation du logiciel ou le site web visité : il est impératif de posséder un antivirus, bien paramétré, et de mettre à jour régulièrement les logiciels et le Système d'Exploitation que l'on utilise.

Pensez aussi à lire la Politique de Confidentialité et les Conditions Générales d'Utilisation ainsi que le message d'avertissement précédent l'installation d'une application. Afin de voir l'étendue des informations que vous laissez sur internet, je vous recommande de lire le très bon article Marc du magazine *Le Tigre*.

Ne soyez pas non plus trop paranoïaques, profitez des opportunités qu'offrent les services du Web 2.0 et Facebook. Il s'agit de progrès assimilables aux autres technologies d'aujourd'hui : ce sont de merveilleux outils, mais à manier avec précaution.

CONCLUSION :

Je vous rappelle tout d'abord que beaucoup de points de vue ici sont applicables au monde des réseaux sociaux en général, et au monde du Web 2.0 plus généralement. Je souhaite bien faire comprendre que l'article réalisé ici ne sert pas à « casser » Facebook ou tout autre service, son but est de sensibiliser les internautes et les inviter à faire attention à leurs données personnelles. Il est fait dans un but constructif, et tout le monde peut y participer en y ajoutant ses idées et remarques.

Il est aussi important de prendre en considération l'évolution de ces réseaux qui séduisent de plus en plus de jeunes, et de moins jeunes. On peut s'attendre à une progression du nombre d'utilisateurs de ces réseaux, et donc à une augmentation du nombre d'attaques ciblant ces réseaux. Il s'agit d'un lieu certes virtuel, mais convivial pour se retrouver : les utilisateurs sont donc en confiance et prennent moins de précautions quant à leurs données personnelles.

Si vous souhaitez me faire part de vos remarques, corrections, idées ou quoique ce soit ou si vous avez apprécié tout simplement cet article, vous pouvez le faire sur ce site : http://www.facebook-danger.fr ou me joindre par mail à l'adresse guig@facebook-danger.fr ou à facebook.danger@gmail.com. J'essaierai d'y répondre le plus rapidement possible. Je suis pour le débat, ainsi, toute remarque est la bienvenue !

REMERCIEMENTS :

Ce projet, aussi modeste soit-il, n'aurait pu se réaliser sans l'aide de plusieurs personnes. Voici donc leur heure de gloire ! Merci à eux tous :

Félix AIMÉ, pour ses réponses, son aide et son soutien : www.felix-aime.fr
Kevin BRUSTIS, pour ses réponses, son soutien et ses conseils précieux : www.kjame.com
Claire GERMOUTY, pour ses réponses, ainsi que
Jérôme BOUTEILLER, pour ses réponses : http://www.jbouteiller.net, co-auteurs du livre *Bienvenue sur Facebook : LE mode d'emploi*
Jacques DUPIN, pour ses relectures et son soutien.
Damien BANCAL, journaliste et fondateur de http://www.zataz.com, pour ses réponses.
Raphaël LABBÉ (*leafar*), pour ses réponses http://www.leafar.eu
Elsa TROCHET MACE Responsable Communication de la CNIL, pour ses réponses.

« FACEBOOK, DANGER ! » - LES SOURCES

- **LES MENACES VIRALES :**

1. http://www.zataz.com/ (le site présente de nombreuses informations sur les failles de sécurité, notamment à propos de Facebook).
2. http://www.topbreakingnewsheadlines.com/news/facebook-error-check-system-beware
3. http://www.generation-nt.com/facebook-photos-faille-securite-byron-actualite-70232.html
4. http://www.cnetfrance.fr/news/internet/une-faille-dans-facebook-permettait-de-voler-les-identifiants-de-connexion-39382901.htm
5. http://www.mag-securs.com/spip.php?article12976
6. http://www.infos-du-net.com/actualite/14983-rapport-cyber-criminalite.html
7. http://pandalabs.pandasecurity.com/archive/Facebook-Phishing-Site-Targets-French-Users.aspx
8. http://www.pcinpact.com/actu/news/49253-comptes-delinquants-sexuels-bannis-facebook.htm
9. http://hadf.wordpress.com/2008/02/13/creer-une-application-facebook-en-java-2/
10. http://www.appinabox.com/
11. http://fr.securityvibes.com/first-cert-facebook-eweek-article-1005.html
12. http://blog.threatexpert.com/

- **LES RISQUES POUR LA VIE PRIVEE :**

1. http://www.infos-du-net.com/actualite/15209-Facebook-vie-privee.html#xtor=RSS-20
2. http://www.infos-du-net.com/actualite/15223-Facebook-vie-privee.html#xtor=RSS-20
3. http://fr.techcrunch.com/2009/02/18/propriete-des-donnees-facebook-retourne-sa-veste/
4. http://www.korben.info/exclu-facebook-va-faire-voter-par-ses-utilisateurs-les-futurs-conditions-generales-de-son-site.html
5. http://www.demainlaveille.fr/2008/12/05/facebook-un-danger-public/
6. http://fjb.blogs.com/weblog/2008/01/les-dangers-de.html
7. http://agora.qc.ca/reftext.nsf/Documents/Facebook--Face_a_face_avec_Facebook_par_Jacques_Dufresne
8. http://www.le-tigre.net/
9. http://www.liberation.fr/societe/0101553055-les-detectives-prives-a-l-heure-de-facebook
10. http://www.cnil.fr/index.php?id=2383

11. http://tempsreel.nouvelobs.com/actualites/societe/20090217.OBS5049/vie_privee_facebook_alarme_ses_utilisateurs.html
12. http://www.zdnet.fr/actualites/internet/0,39020774,39372774,00.htm
13. http://www.ecrans.fr/-Web-2-gare-a-vos-traces-.html

- **PRESENTATION :**

1. http://blog.lefigaro.fr/hightech/2009/02/pourquoi-twitter-ne-va-pas-cha.html
2. http://docs.justia.com/cases/federal/district-courts/california/candce/5:2007cv01389/189975/474/0.pdf
3. http://www.infos-du-net.com/actualite/15186-pdf-surcote-facebook.html#xtor=RSS-20
4. http://www.korben.info/et-pendant-ce-temps-la-que-font-nos-ados.html
5. http://fr.techcrunch.com/2009/02/17/fr-les-francais-aiment-les-reseaux-sociaux-et-facebook-depasse-skyrock/
6. http://www.mediametrie.fr/index.php
7. http://www.comscore.com/press/release.asp?press=2725
8. http://www.yoolink.fr/tag?word=facebook&search_topic=2
9. http://fr.techcrunch.com/2009/02/23/10-milliards-de-photos-sur-facebook/
10. http://www.taxiclic.com/questions/quelle_est_l-histoire_de_facebook-733.html
11. http://fr.wikipedia.org/wiki/Facebook
12. http://www.infos-du-net.com/actualite/15254-Facebook-Gamelin-salaries.html#xtor=RSS-20

- **SE PROTEGER :**

1. http://www.korben.info/facebook-supprimer-son-compte.html
2. http://www.korben.info/10-conseils-pour-eviter-de-petits-ennuis-avec-sa-vie-privee-sur-facebook.html