



GUIDE PRATIQUE

Les dangers de Facebook,
Comment bien sécuriser son profil
L'accès aux fonctions cachées de
Facebook

Jean-Philippe NOAT
Directeur Technique



Vue la montée en puissance des réseaux sociaux chez les ados et en entreprise le premier thème de nos guides pratiques s'est naturellement fait jour sur le principal réseau social utilisé en 2009 / 2010 : Facebook. (300 millions d'utilisateurs dont 50 dans les deux derniers mois).

Les principaux dangers sont le vol d'identité et la perte en termes d'image. Dans nos sessions de prévention, nous vous expliquerons comment vous en protéger.

Dans un registre plus léger, mais hélas réel, nous vous donnons des exemples de dérive qui resteront dans les annales.

L'objectif est de se rendre compte que si Internet a tendance à déshumaniser les contacts, et, de fait, incite à plus de libertés les dangers sont là sur la Toile et mieux vaut rester sur ses gardes comme dans la vraie vie.

Facebook déclenche les passions : certains ont déjà tous les symptômes de la dépendance et y passent des heures chaque jour tandis que d'autres ne lui trouvent qu'un intérêt négligeable voire inexistant.

Quoiqu'il en soit Facebook contribue fortement au vent qui souffle sur la Toile aussi appelé web 2.0. Seulement ce vent là annonce la tempête. En effet tout comme d'autres réseaux sociaux son utilisation présente des risques pour la sécurité des utilisateurs, et par leur biais, des entreprises.

Ce site est dénoncé par de nombreuses organisations non gouvernementales de défense des droits de l'homme, des pétitions circulent, des groupes se créent dénonçant cette violation de la vie privée. Le danger principal vient cependant de l'utilisateur lui-même ! Trop souvent hélas les utilisateurs n'ont pas conscience de l'importance des informations qu'ils publient sur Internet qui n'est autre que la porte d'entrée mondiale vers leur vie privée et personnelle...

Pour illustrer ces propos, nous allons prendre l'exemple de Freddi Staur (anagramme de « ID Frauster »), le profil créé pour les besoins de l'enquête de Sophos (société spécialisée dans la sécurité d'Internet). A partir de ce profil, 200 « invitations » ont été envoyées pour accepter Freddi comme ami, ces invitations pouvant être acceptées ou refusées par les destinataires. Résultat : 41% des utilisateurs de Facebook ont accepté l'invitation et sont devenus « amis » avec Freddi Staur et ont donc accepté de lui divulguer leurs données personnelles. Freddi a ainsi pu récupérer leur email, date de naissance, numéros de téléphone, photos de famille ou d'amis, leurs goûts, hobbies, religion et bien d'autres données privées. Cette enquête met parfaitement en lumière le comportement totalement irresponsable des utilisateurs des réseaux sociaux.

Ce qui surprend et inquiète c'est de constater avec quelle facilité la plupart des utilisateurs divulguent leurs informations... à des inconnus alors qu'ils refuseraient dans la vraie vie de les communiquer -et à juste titre- à un inconnu dans la rue. Freddi aura ainsi obtenu assez d'information pour créer des messages de phishing ou des programmes malveillants personnalisés, deviner des mots de passe ou

usurper l'identité des nouveaux « amis ». Il a toutes les armes en main pour devenir un parfait cybercriminel.

A savoir

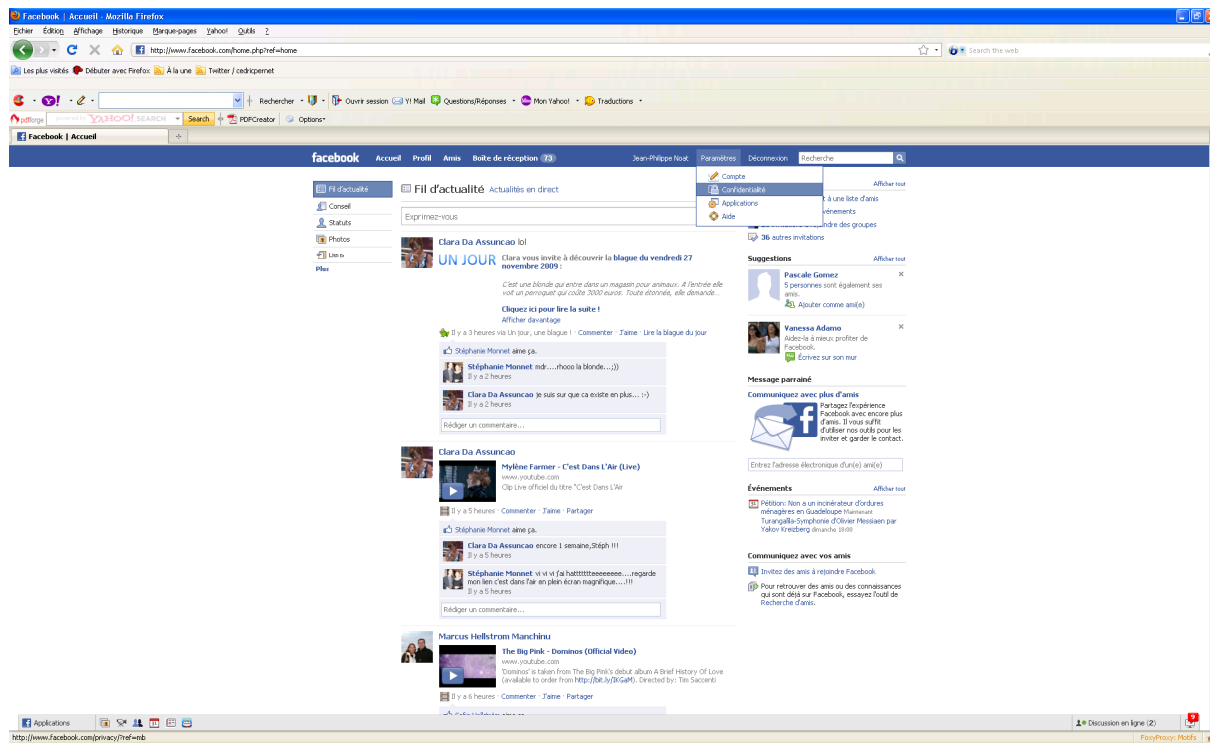
- **Un utilisateur britannique sur trois** a recherché sur des sites comme Facebook des informations sur son patron, ses collègues, ou des candidats à un emploi (source étude du gouvernement britannique pour la campagne « Get safe online »).
- Malgré toute l'attention portée aux intrusions et aux virus il y a **72% de malchance** que la prochaine attaque réussie provienne de l'intérieur de l'entreprise (source EuroCACS conférence européenne sur les politiques de sécurité).
- Plus **d'un million d'ordinateurs seraient** sous l'influence de robots capables d'envoyer **100 milliards de spam** par jour (source RSA conference 2008).
- **Un quart des utilisateurs britanniques** des sites de réseaux sociaux comme Facebook révèlent des informations sensibles sur leurs profils comme leurs coordonnées (adresse postale, téléphone), leur date de naissance ou leur religion (source étude du gouvernement britannique pour la campagne « Get safe online »).

Les dérives de Facebook

- Monsieur S. planificateur financier respectable de Montréal a eu la curieuse idée de mettre pour photo de profil : lui-même... travesti en infirmière blonde... Il a perdu son emploi, son employeur ayant vu son profil Facebook.
- Monsieur L, conseiller financier (contrairement à sa photo qui le montrerait plutôt culturiste ou escort boy) on peut y lire le moindre détail de sa vie, ce qu'il mange, ses films préférés et les photos de ses conquêtes... cela lui a valu un divorce.
- Tout comme les soldats américains en Irak, des soldats de Tsahal, l'armée israélienne, se sont affichés sur Facebook révélant décors et paysage des bases secrètes de l'armée...avec les conséquences que l'on imagine.
- Un jeune étudiant, Adam Morisson a été soupçonné de vouloir commettre une tuerie en raison d'informations publiées en utilisant sa photo prise sur Facebook. Son identité et sa photo ont été utilisées pour créer un faux compte et annoncer la tuerie. L'étudiant s'est retrouvé interrogé par la police et en garde à vue.
- Une faille de sécurité sur Facebook a rendu accessible à tous les photos de certains utilisateurs paramétrées pour n'être visibles qu'aux amis... dont celles du fondateur de Facebook : Mark Zuckerberg.

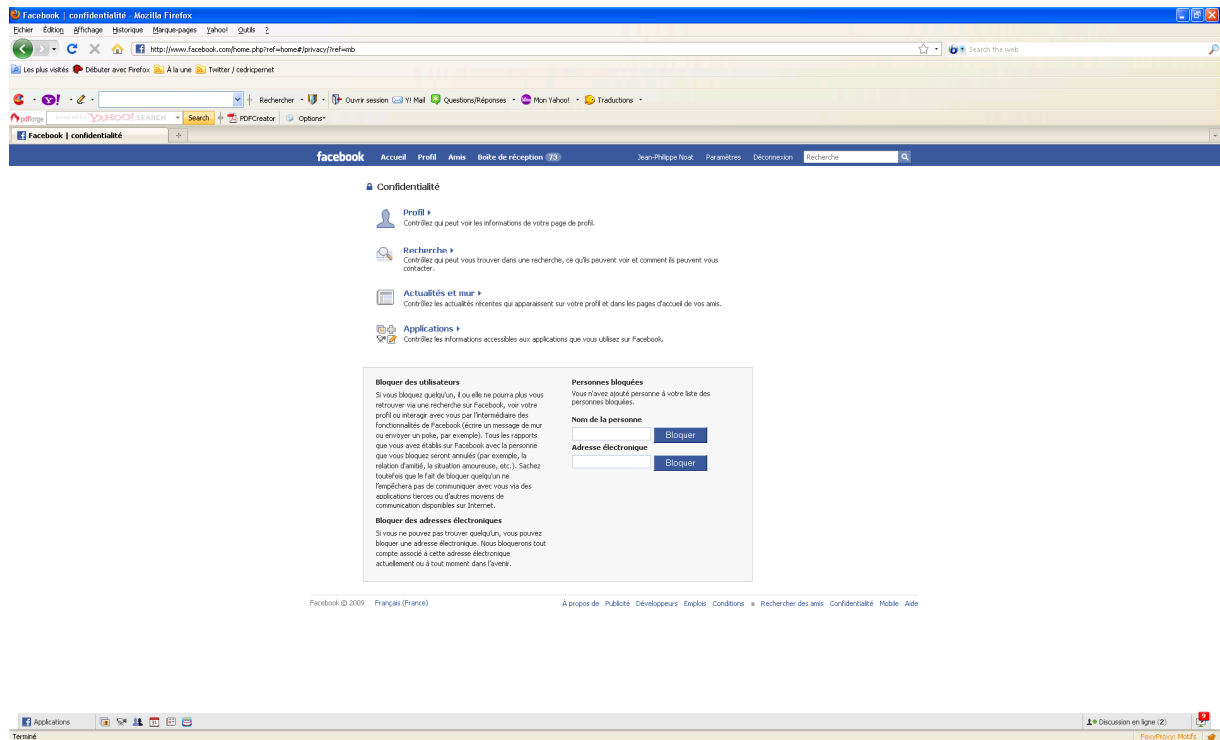
Sécuriser au mieux son Facebook

Pour paramétrer les options de confidentialité de Facebook, cliquez sur Confidentialité en haut à droite de la fenêtre.



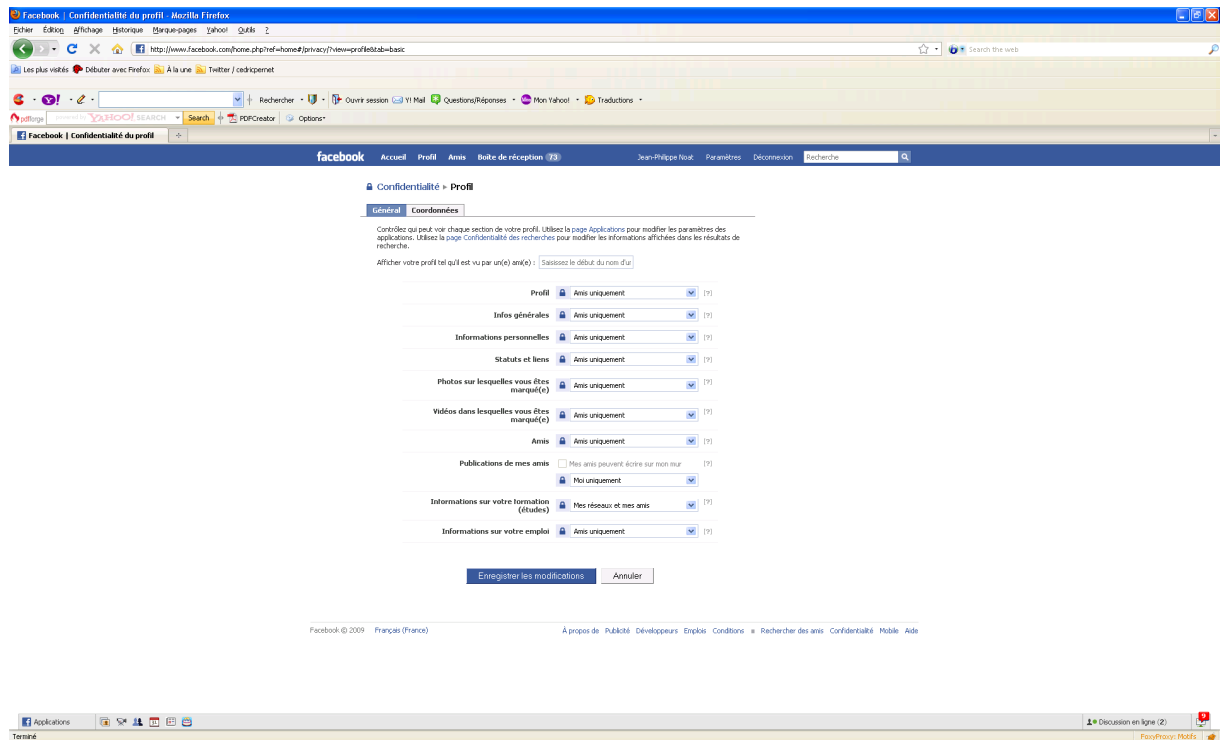
On accède alors à l'écran suivant :





Chaque module présente des options à paramétrer. Nous allons les passer en revue une à une. Nous en expliquerons les fonctions, puis, nous vous recommanderons des paramétrages afin d'allier au mieux l'aspect ludique de Facebook à la protection de votre identité.

Note : N'oubliez pas de cliquer sur le bouton « Enregistrer les modifications / Save Changes » après chaque paramétrage afin qu'il soit pris en compte.



L'option **Profil /Profile** permet de choisir qui peut voir votre profil.

Attention : Si vous n'avez pas intégré de réseau, cette option est réglée par défaut sur « Seulement mes amis » / « Only Friends ». Seulement, dès que vous rejoignez un réseau, par exemple, le réseau Monaco, ce paramétrage par défaut se change en « Mes réseaux et mes amis » / « My Networks and Friends » et votre profil est accessible à l'intégralité de votre (ou vos) réseau(x) ... parmi le(s)quel(s) peuvent se trouver des voleurs d'identité !

L'option « **Information générales** » permet de gérer qui, en consultant votre profil, pourra également voir vos informations générales : votre sexe, date de naissance, ville natale, opinions politique, religion et situation amoureuse.

Attention : On ne peut pas mettre moins que la notion générique « d'amis » pour accéder aux informations personnelles. Le terme d'ami sur Facebook a donc des conséquences très lourdes sur l'accès aux informations dites personnelles ou confidentielles. Il y a donc bien lieu de mettre le moins possible d'informations personnelles sur ce média.

A savoir : Ces informations peuvent être utilisées par des pirates ou des publicitaires ou/et peuvent nuire à votre image.

L'option « **Informations personnelles** » permet de choisir qui, en consultant votre profil, pourra voir vos Informations personnelles, lesquelles comprennent vos Intérêts, Activités, Favoris (musique, films, etc.) et votre section À propos de moi.



L'option « **Status et Liens** » permet de décider qui peut voir les mises à jour de votre statut, c'est-à-dire la petite phrase écrite à côté de votre nom qui ne manque souvent pas d'humour. Citons un exemple des plus illustratifs : « X laisse pousser sa barbe pour le concert de ZZ Top ! ».

A savoir : Tout comme l'exemple cité, les statuts sont souvent amusants (voire saugrenus), mais peuvent aussi être dangereux du fait qu'ils puissent être utilisés par des malfaiteurs : « 2 semaines de vacances bien méritées » + adresse publiée ou une rapide recherche sur un annuaire du web bien connu à partir de vos nom et prénom...et l'affaire est dans le sac !

L'option « **Photos sur lesquelles vous êtes taggué(e)** » permet de décider qui pourra voir les photos que vous-même ou vos amis avez « tagguées ».

A savoir : Se retrouver « taggué » après une soirée trop arrosée peut avoir quelques conséquences...surtout si vos supérieurs et collègues de bureau ont accès à ces photos ! Sachez que, par **défaut, tous vos réseaux et vos amis y ont accès.**

L'option « **Vidéos sur lesquelles vous êtes taggué(e)** » permet de décider qui pourra voir les vidéos que vous-même ou vos amis avez « tagguées ».

A savoir : Se retrouver « taggué » après une soirée trop arrosée peut avoir quelques conséquences...surtout si vos supérieurs et collègues de bureau ont accès à ces vidéos ! Sachez que, par **défaut, tous vos réseaux et vos amis y ont accès.** Des personnes ont déjà perdu leur emploi par le biais de cette fonctionnalité.

L'option « **Amis** » permet de décider qui peut voir la liste de vos amis.

A savoir : **En accédant au profil de vos amis, un usurpateur d'identité pourrait avoir accès à des informations vous concernant surtout si ceux-ci (contrairement à vous !) n'ont pas configuré les paramètres de confidentialité de manière adéquate. C'est donc une réelle prise de conscience qui vous est conseillée ici. L'accès à vos informations personnelles peut dépendre d'un ami qui lui aura peu ou pas sécurisé son Facebook.**

L'option « **Publication de mes amis** » est utilisée pour décider qui, en consultant votre profil, pourra voir les messages de votre mur publiés par vos amis.

A savoir : le degré d'"intimité" de vos échanges sur le mur, en plus de nuire à votre réputation, peut être utilisé par des pirates. Par défaut, cette option est réglée sur « Mes réseaux et amis ». Le conseil d'Action Innocence est de mettre sur « moi seulement » afin de préserver l'accès à ces informations.

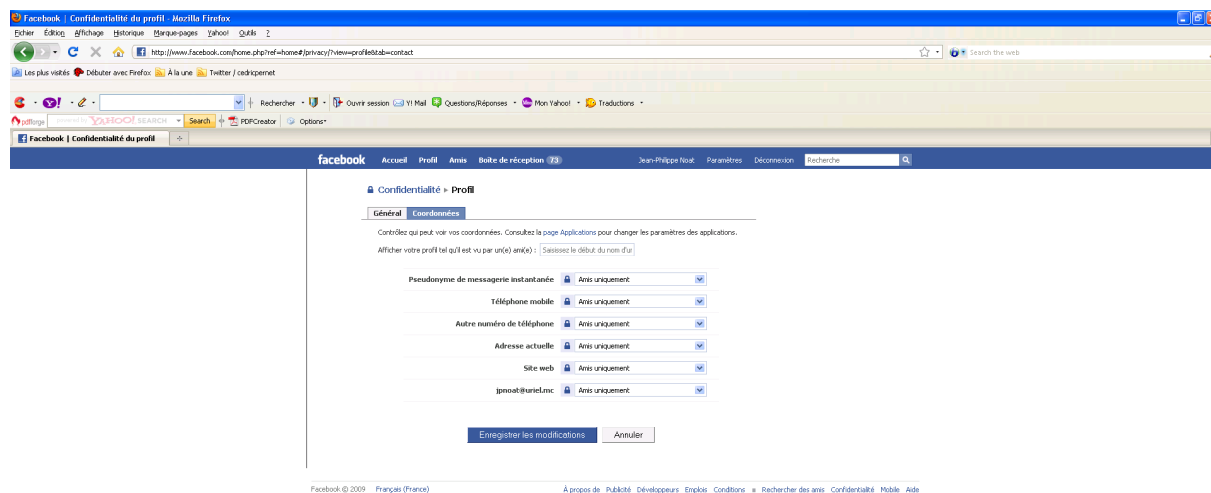
L'option « **Information sur votre formation (études)** » permet de décider qui, parmi ceux autorisés à accéder à votre profil, pourra voir vos informations concernant votre cursus scolaire.

A savoir : Par défaut, cette option est réglée sur « Seulement mes amis »

L'option « **Information sur votre emploi** » permet de décider qui, parmi ceux que vous avez autorisé à accéder à votre profil, pourra voir les informations concernant votre emploi.

A savoir : Par défaut, cette option est réglée sur « Seulement mes amis »

On clique maintenant sur la partie « **Coordonnées** » du profil



L'option « **Pseudo de messagerie instantanée** » permet de filtrer qui a accès à mon adresse de messagerie instantanée (chat).

Recommandation Action Innocence : Ne pas remplir ce champ : les vrais amis auront l'information directement par mon intermédiaire et pas par l'intermédiaire de ce site.

L'option « **Téléphone mobile** » permet de filtrer qui a accès à mon numéro de mobile.

Recommandation Action Innocence : Ne pas remplir ce champ : les vrais amis auront l'information directement par mon intermédiaire et pas par l'intermédiaire de ce site.

L'option « **Autre Numéro de Téléphone** » invité l'utilisateur à saisir un 2^{ème} numéro de téléphone (en plus du numéro de mobile déjà proposé).



Recommandation Action Innocence : Ne pas remplir ce champ : les vrais amis auront l'information directement par mon intermédiaire et pas par l'intermédiaire de ce site.

L'option « **Adresse actuelle** » invite l'utilisateur à saisir son adresse personnelle.

Recommandation Action Innocence : Ne pas remplir ce champ : les vrais amis auront l'information directement par mon intermédiaire et pas par l'intermédiaire de ce site.

A savoir : Vos amis devraient connaître votre numéro de téléphone mobile et savoir où vous habitez. En cas d'oubli ou perte, ils peuvent toujours vous contacter via Facebook pour vous les demander.

L'option « **Site web** » invite l'utilisateur à rentrer son site web personnel ou l'adresse de son blog.

A savoir : Il va sans dire que si votre site web contient des informations personnelles, le mieux est de choisir le paramétrage de niveau « optimal » (voir Tableau des recommandations).

L'option « **Adresse email** » : xxx@xxx.com attend de l'utilisateur la saisie de son adresse mail.

A savoir : Sur Facebook, vos amis peuvent vous envoyer des messages sans connaître votre adresse électronique. Alors pourquoi publier votre adresse mail ?

Plus généralement les options de cette partie doivent être configurées au minimum et si possible ne pas être renseignées.

Tableau de synthèse

	Option	Module Profil								
		Mes réseaux et mes amis	Ami(e)s d'ami(e)s	Seulement mes amis	Personne	Personnaliser				
						Aucun de mes réseaux				Certains/tous mes réseaux
						Ami(e)s d'ami(e)s	Seulement mes amis avec "Excepté ces personnes" (1)	Certains amis puis ajouter leurs noms ou une liste (2)	Seulement moi	
Basique	Profil			+++						
	Infos de base			+						
	Informations personnelles			+						
	Mises à jour du statut			+						
	Photos sur lesquelles vous êtes taggué(e)			+						
	Vidéos sur lesquelles vous êtes taggué(e)			+						
	Amis			+						
	Mur			+						
	Parcours scolaire/universitaire Infos professionnelles			+						
Coordonnées	Pseudo de messagerie instantanée				+					
	Téléphone mobile/Ligne fixe				+					
	Adresse actuelle				+					
	Site web			+... avec prudence (3)						
	xxx@xxx.com			N	+					

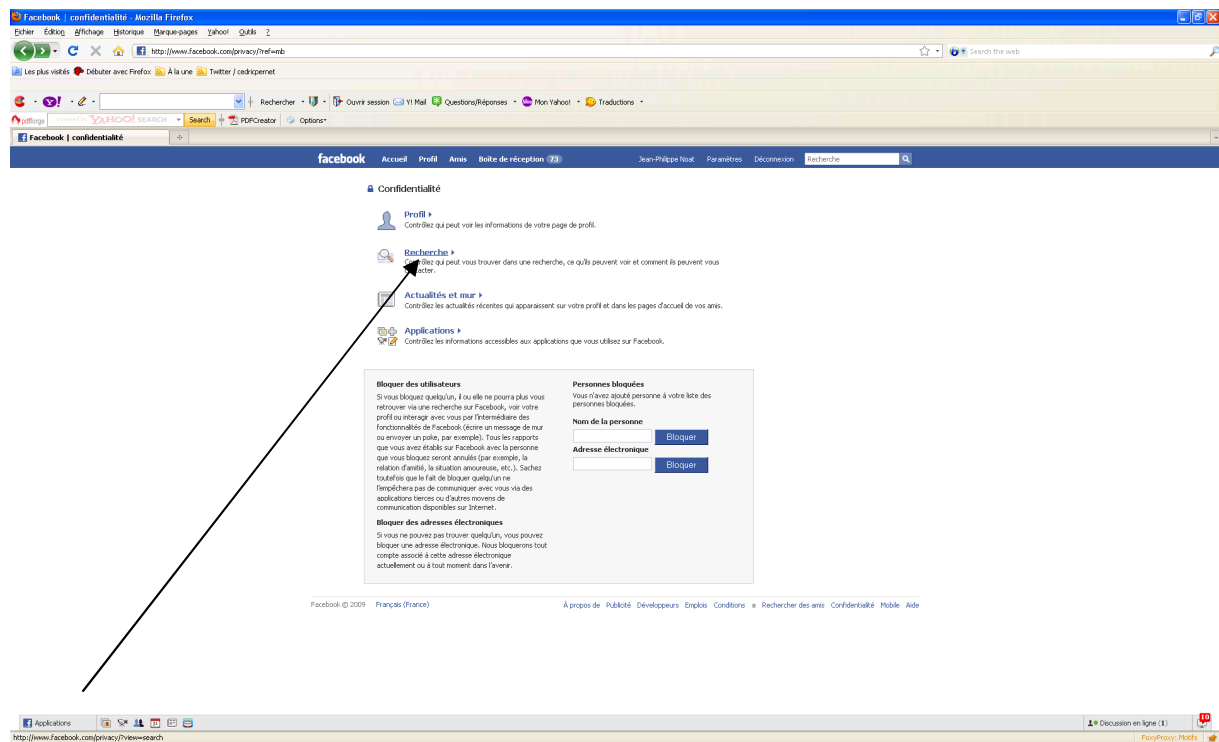
	Déconseillé
+	Niveau Minimum
++	Niveau Correct
+++	Niveau Optimal

	Ce paramétrage n'existe pas pour cette option
	Ne présente que peu d'intérêt

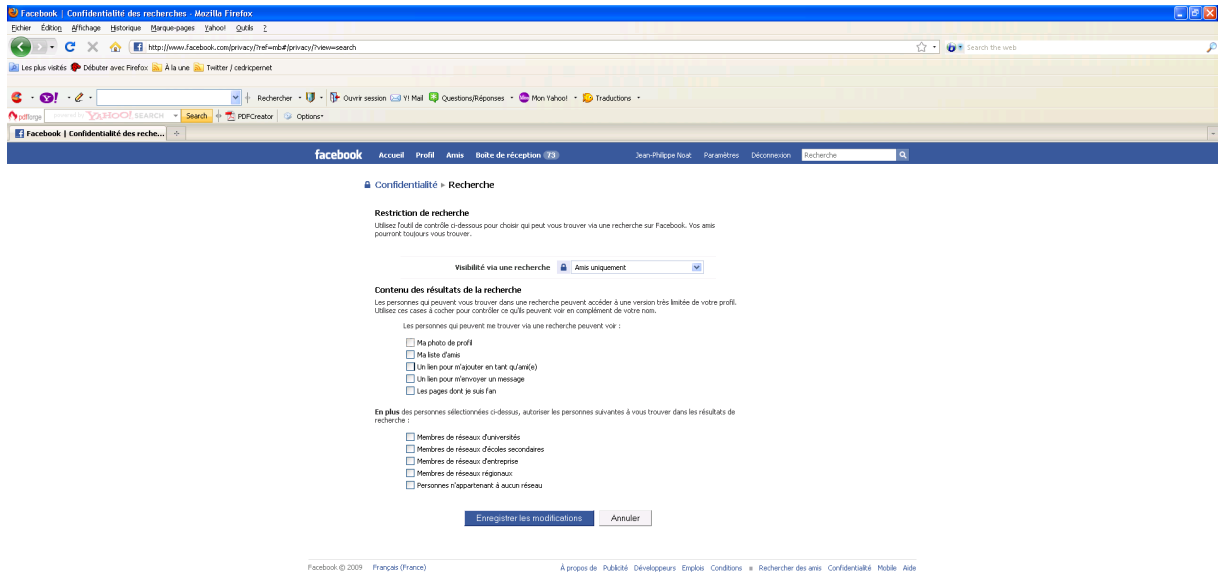
(1) « Excepté ces personnes » (« Except these People ») permet de soustraire de votre liste d'amis ceux dont vous ne souhaitez pas qu'ils aient accès à certaines de vos informations. Vous pouvez aussi enlever de votre liste d'amis, une sous-liste d'« amis » que vous aurez préalablement créée, par exemple, une liste des « amis » n'ayant pas accès à vos photos (voir Annexe : Comment créer une « limited list »).

(2) En choisissant Certains amis (Some Friends) puis en tapant le nom des « amis » dont vous souhaitez qu'ils aient accès à ces informations permet, vous aurez un contrôle parfait sur vos informations. En effet, vous ajouterez au fur et à mesure les « amis » pouvant avoir accès à vos informations. Ainsi, si vous négligez d'ajouter un « ami », les conséquences seront certainement moindres que si vous oubliez d'ôter un « ami » indésirable de votre liste (voir note 1 ci-dessus). En outre, vous pouvez ajouter une sous-liste d'« amis » autorisés à accéder à certaines informations, par exemple, une liste des « amis » ayant accès à votre Wall (voir Comment créer une « limited list »)

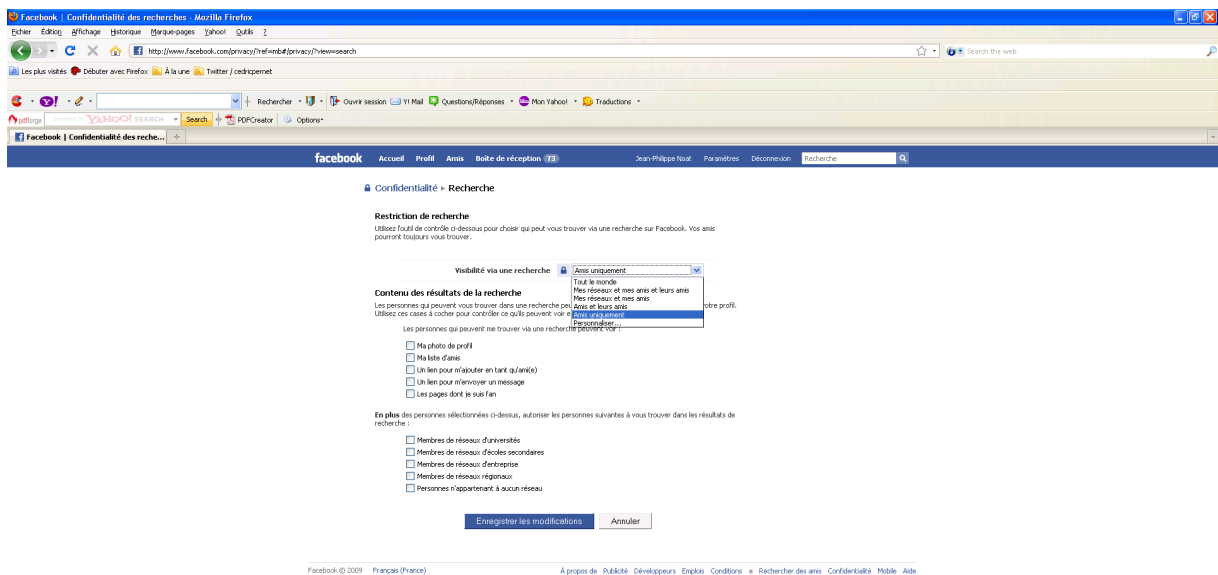
(3) Il va sans dire que votre site Web ne doit pas exposer vos données personnelles.



Cliquer maintenant sur la partie « Recherche » des options de confidentialité.



Il s'agit là d'une option extrêmement importante car elle va conditionner notre visibilité non seulement dans Facebook mais plus généralement dans les moteurs de recherche au sens large (Google par exemple).



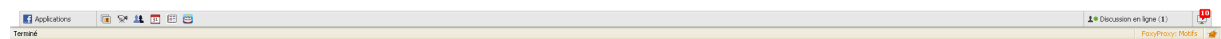
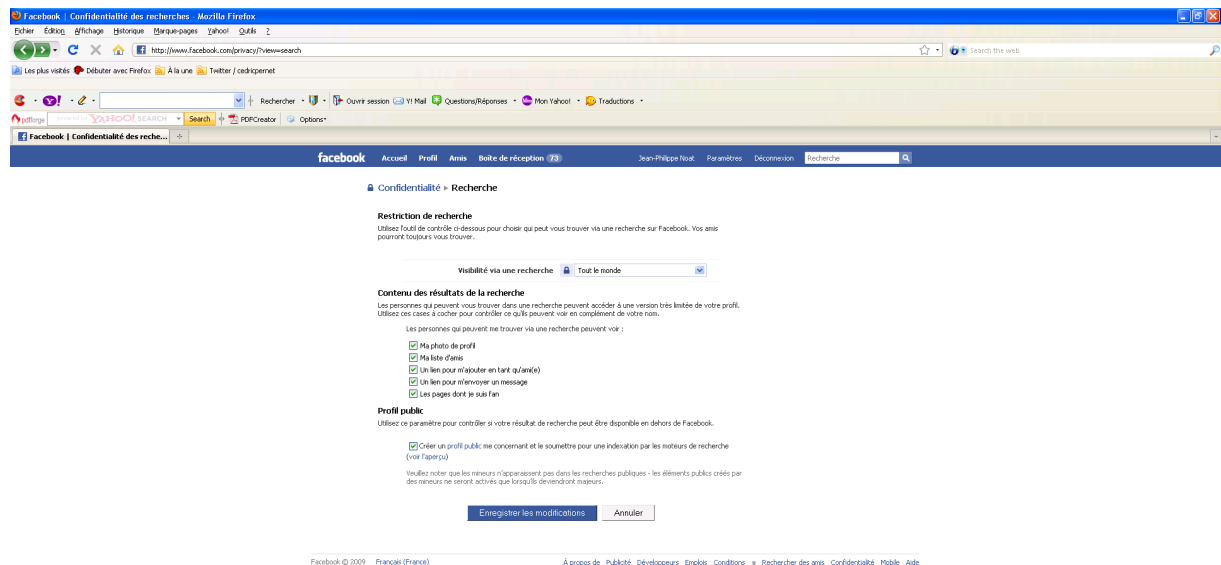
La première option à paramétrer consiste à modifier le paramètre « **visibilité sur une recherche** ». Par défaut ce paramètre est fixé sur « Tout le monde ». On peut



comprendre que bloquer ce paramètre sur « Amis uniquement » permet de nous rendre difficilement visible depuis Facebook (ce qui est précisément le but inverse du réseau social). Un bon compromis peut être alors « Amis et leurs amis » ou « Mes réseaux et mes amis ».

Le « **contenu du résultat de recherche** » est à paramétrer beaucoup plus finement tant les informations sont nombreuses et accessibles par défaut.

Voici les options de Facebook par défaut :

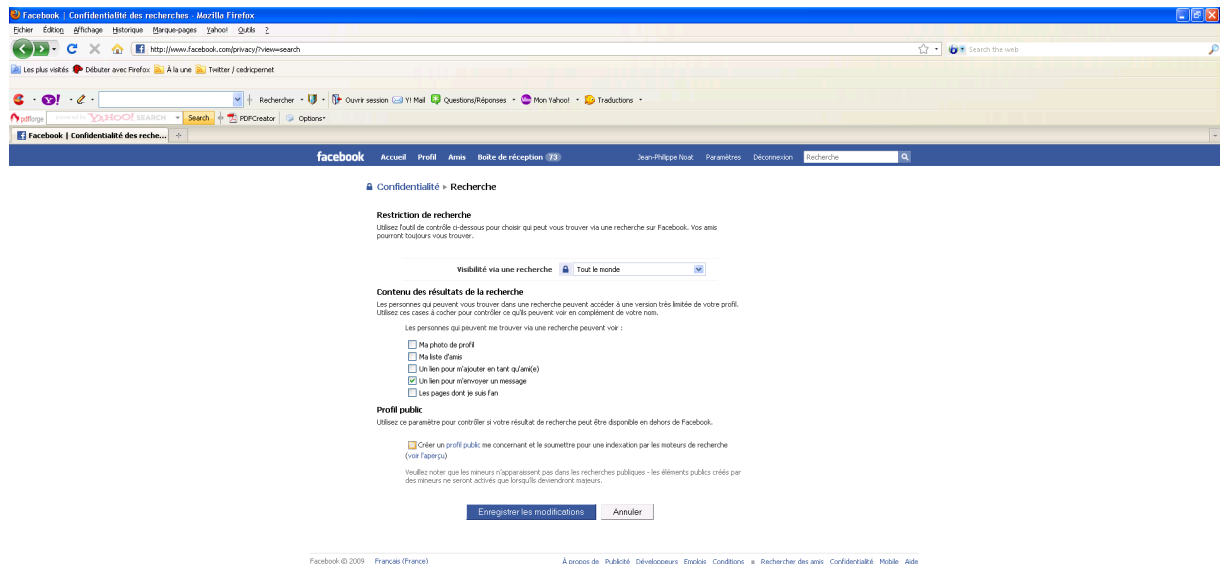


L'option « **Profil public** » permet de créer un profil public et de l'indexer dans les moteurs de recherche tels que Google ou Yahoo.

A savoir : Si cette option est activée (et elle l'est par défaut !), tout internaute faisant une recherche à partir de vos nom et prénom sur Google, Yahoo ou autres pourra voir votre « profil public » composé, en plus de vos nom et prénom, de votre photo et de celle de cinq de vos amis, donc attention au choix de votre photo et ...à celui de vos amis! Vous pouvez faire l'expérience en tapant votre propre nom sur Google ou Yahoo.

Recommandation : Décochez l'option Profil public

Attention ! Cette option a tendance à se réactiver automatiquement à chaque changement de paramètre !!! Veillez donc bien à la désactiver.



Écran de paramétrage recommandé :

- ne pas mettre sa photo par défaut sur les recherches (si les personnes ont besoin de me voir elles doivent d'abord m'envoyer un message). La photo de moi peut indiquer mon âge, mon lieu d'habitation et des informations personnelles à mon insu.
- ne pas laisser voir sa liste d'amis (cela ne regarde que moi et une personne externe n'a pas à voir mes amis tant qu'elle ne me connaît pas).
- ne pas envoyer de lien pour le rajouter en tant qu'ami (ne pas oublier que par défaut je ne connais pas la personne qui fait la recherche sur Facebook).
- un lien pour m'envoyer un message (sans communiquer mon adresse personnelle de courriel je peux utiliser Facebook pour communiquer et là c'est un avantage et un point fort).
- les pages dont je suis fan (et donc qui peuvent révéler des informations, lieu d'habitation, photos de moi ou de mes copains etc....) il est donc souhaitable de décocher cette option.

Attention : Si vous choisissez de cocher « Vous envoyer un message », une personne n'ayant pas accès à votre profil peut alors vous envoyer un message. Dans ce cas, **si vous choisissez d'y répondre soyez conscient des risques**. En effet, si vous répondez au message d'un inconnu en laissant les paramètres par défaut, celui-ci pourra voir la photo de votre profil, la liste de vos amis et vos informations de base – sexe, date de naissance, opinions politiques, parcours scolaire et universitaires et parcours professionnelles...ainsi que le ou les réseaux au(x)quel(s) vous avez adhéré(s). Il peut alors pousser le vice plus loin et intégrer votre réseau pour accéder à encore plus d'informations telles que vos articles, vos éléments publiés, vos groupes, votre Super Wall (si vous avez laissé le paramétrage par défaut – voir le module Applications),...les photos ne semblent pas accessibles,

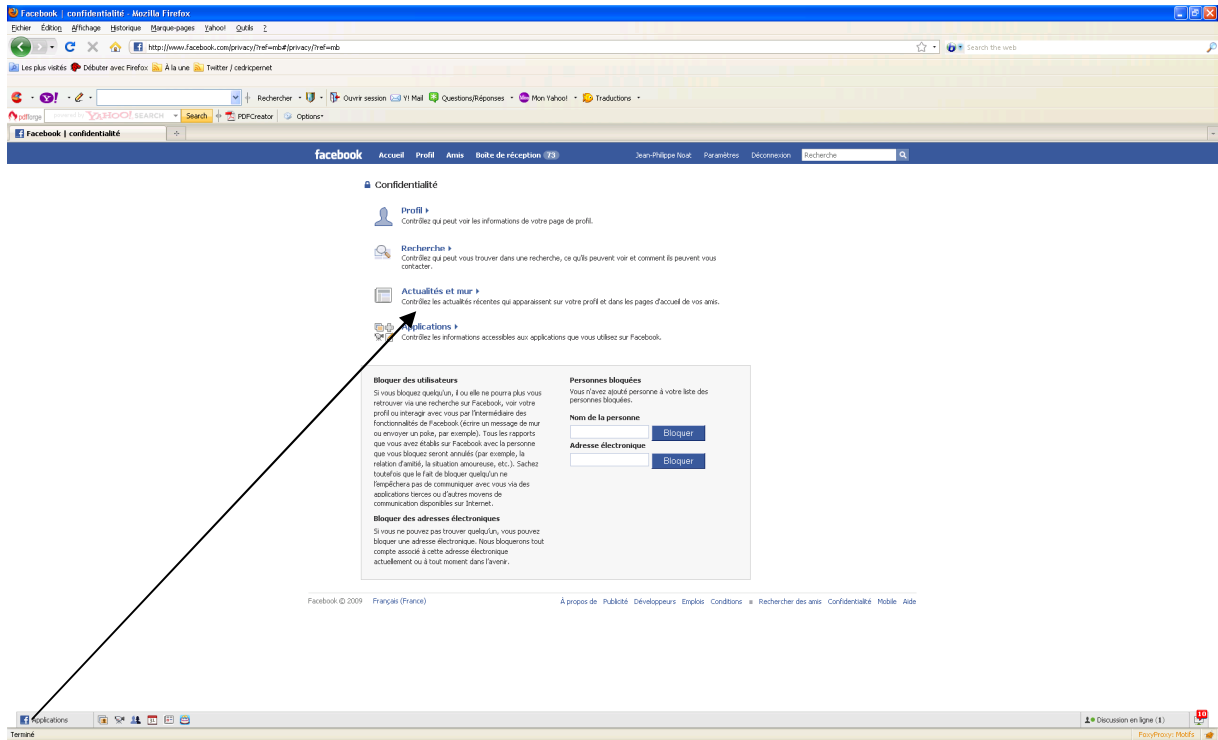
pourtant, si elles se trouvent dans vos Mini-news, il suffit de cliquer dessus pour y accéder !

Voici par exemple ce qu'un inconnu peut voir avec le paramétrage par défaut :

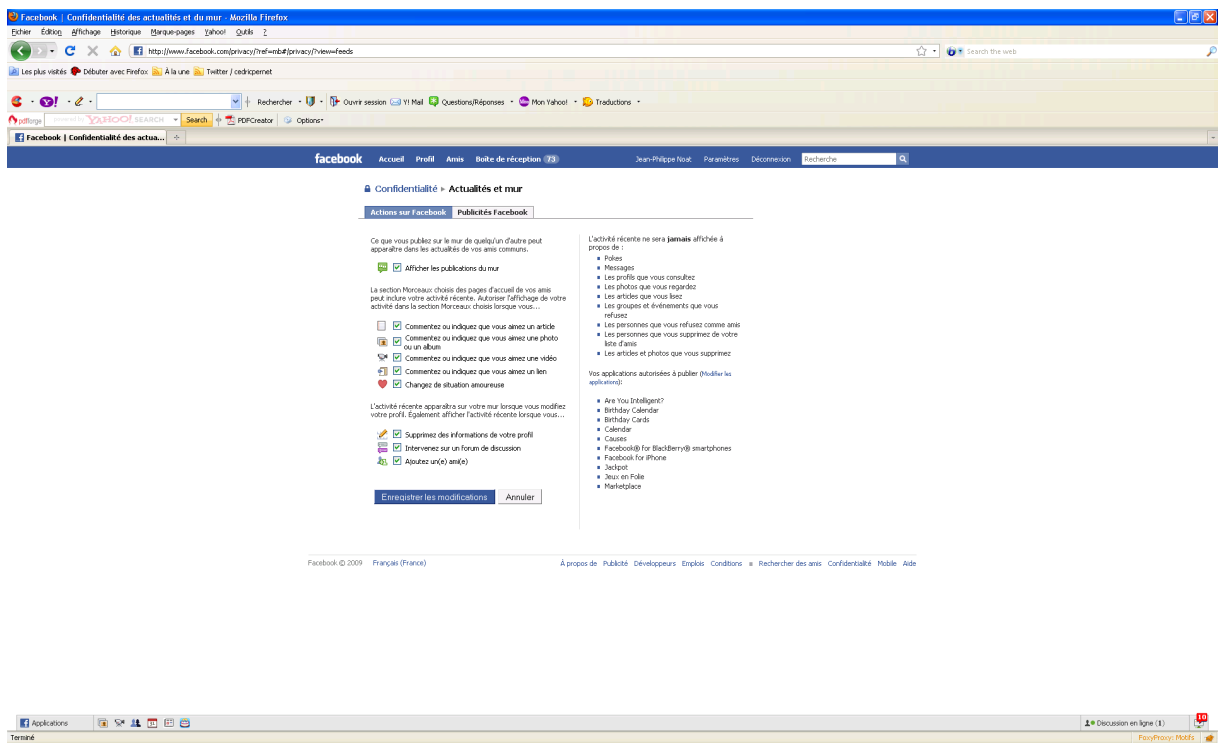


Une dernière « curiosité » : même si vous avez paramétré l'option Amis du module Profil à « Seulement mes amis » (voir le module Profil), **vos amis sera visible par l'inconnu en question.**

Conclusion : mieux vaut ne jamais répondre à un message ou un pike provenant d'un inconnu. Eh oui, ceci est valable pour les pokes (en retournant un pike à un inconnu, celui-ci aura accès aux informations de votre profil qui ne sont pas protégées par un bon paramétrage et même lors d'une Friend Request...mais là, c'est moins grave, puisque vous êtes censé savoir à qui vous souhaitez l'adresser ! S'il est déjà trop tard, **bloquez l'indésirable**, il ne pourra ainsi plus accéder à votre profil en cliquant sur votre nom inscrit sur le message puisque le lien aura disparu (voir : **Comment bloquer des « amis » ou des inconnus indésirables**).



On clique maintenant sur la partie « Actualités et Mur ».

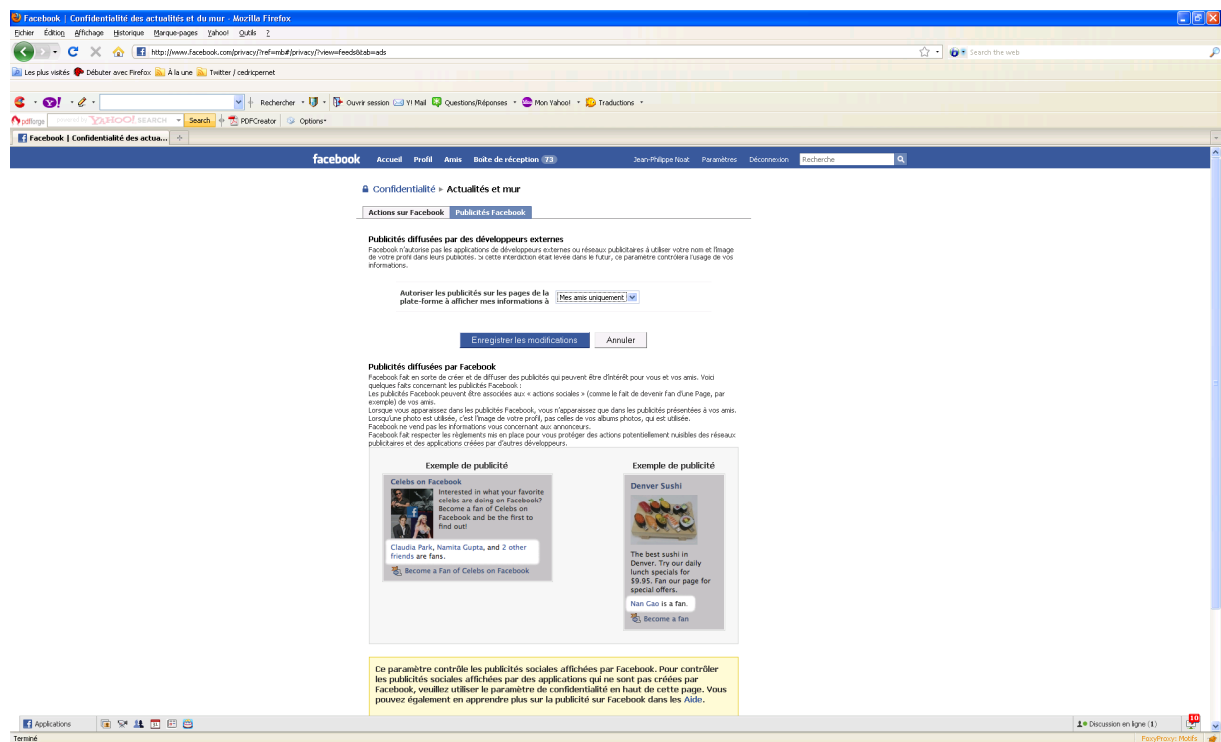


Vous pouvez choisir dans cette partie comment vos amis sont avertis de vos actions dans Facebook et quelles actions doivent leur être indiquées. Tout dépend dans ce cas du nombre d'amis et du degré d'intimité de vos amis.



A ce niveau là il est important de distinguer un ami « virtuel » qui ne me connaît pas et qui ne m'a jamais vu d'un ami « réel » dans la vraie vie qui lui me connaît et peut avoir accès à des informations plus personnelles.

En outre, si vous avez laissé les paramètres par défaut de vos applications, les actions que vous effectuez via celles-ci seront publiées dans votre Mini-news et les News de vos amis. Vos amis pourront alors lire, dans leur News, les « histoires » de vos applications, par exemple, pour le FunWall, « X has just sent a new Post ». Pour contrôler si les actions que vous faites via vos applications seront visibles ou pas dans vos Mini-news et les News de vos amis, cliquez sur Modifier les applications (1) et rendez-vous dans le module Applications pour le détail des paramètres de confidentialité.



Par défaut les publicités qui vous toucheront sur Facebook (via une application ou un message, toucheront également vos amis). Le seul moyen d'éviter cela est de cliquer sur l'onglet « personne » dans cet écran.

Les applications dans Facebook

Contrôlez les informations auxquelles les applications que vous utilisez sur Facebook peuvent accéder et partager depuis votre profil. Ce module permet, non seulement, de supprimer vos applications inutiles, mais aussi, de modifier les paramètres de confidentialité de vos applications. Avant de passer en revue les paramètres de confidentialité de ce module, nous allons exposer quelques informations et conseils qui pourraient s'avérer utiles lors de l'ajout d'une nouvelle application.

Mesures à prendre lors du rajout d'une application dans Facebook

Ajouter Super Wall à votre compte Facebook ?

Super Wall par RockYou!

Autoriser cette application à...

- Savoir qui je suis et accéder à mes informations
- Ajouter une boîte dans mon profil
- Placer un lien dans la colonne de navigation de gauche
- Publier des articles dans mes News et mes Mini-news
- Placer un lien sous la photo de chaque profil
- M'envoyer des notifications par e-mail

Super Wall n'a pas été créée par Facebook. En cliquant sur Ajouter, vous acceptez également les [Conditions d'utilisation des applications](#) de la plate-forme.

Ajouter Super Wall
ou annuler

Description du développeur
« Share videos, pictures, graffiti, and more with your friends! »
[Plus d'infos sur Super Wall](#)

Classement
★★★★☆ (2.8 sur 5)
Sur la base de 257 avis

Vous craignez des abus de la part de cette application ?
[Bloquer Super Wall](#)

Par défaut 6 cases sont cochées.

En particulier l'option 1 : « savoir qui je suis et accéder à mes informations » permet au développeur de l'application d'accéder non seulement à mon profil mais également à celui de mes amis.

Le problème est que pour que l'application soit installée sur votre profil, vous devez, la plupart du temps, laisser cocher la case « Savoir qui je suis et accéder à mes informations », ce qui signifie que vous « partagez » une partie de vos données personnelles – date de naissance, adresse, numéro de téléphone, situation professionnelle ou autres - avec l'auteur de l'application...que vous ne connaissez certainement pas !

Savoir qui je suis et accéder à mes informations

Il est **nécessaire** d'autoriser l'accès aux informations personnelles pour ajouter de nouvelles applications. Si vous ne souhaitez pas autoriser l'accès à vos informations personnelles, **n'ajoutez pas cette application.**

Ajouter une boîte dans mon profil

Placer un lien dans la colonne de navigation de gauche

Publier des articles dans mes News et mes Mini-news

Placer un lien sous la photo de chaque profil

M'envoyer des notifications par e-mail

Super Wall n'a **pas été créée par Facebook**. En cliquant sur Ajouter, vous acceptez également les Conditions d'utilisation des applications de la plateforme.

ou annuler

★★★★★ (2,8 sur 5)
Sur la base de 257 avis

Vous craignez des abus de la part de cette application ?
[Bloquer Super Wall](#)

A savoir : Des applications à l'aspect inoffensif telles des quizz farfelus - « quel animal êtes-vous ? », « Quelle courgette êtes-vous ? » - peuvent être de véritables « aspirateurs » de données...l'auteur de l'application peut alors se constituer une solide base de données à moindre frais ou même les utiliser afin d'usurper votre identité pour, par exemple, ouvrir un compte en banque à votre nom.

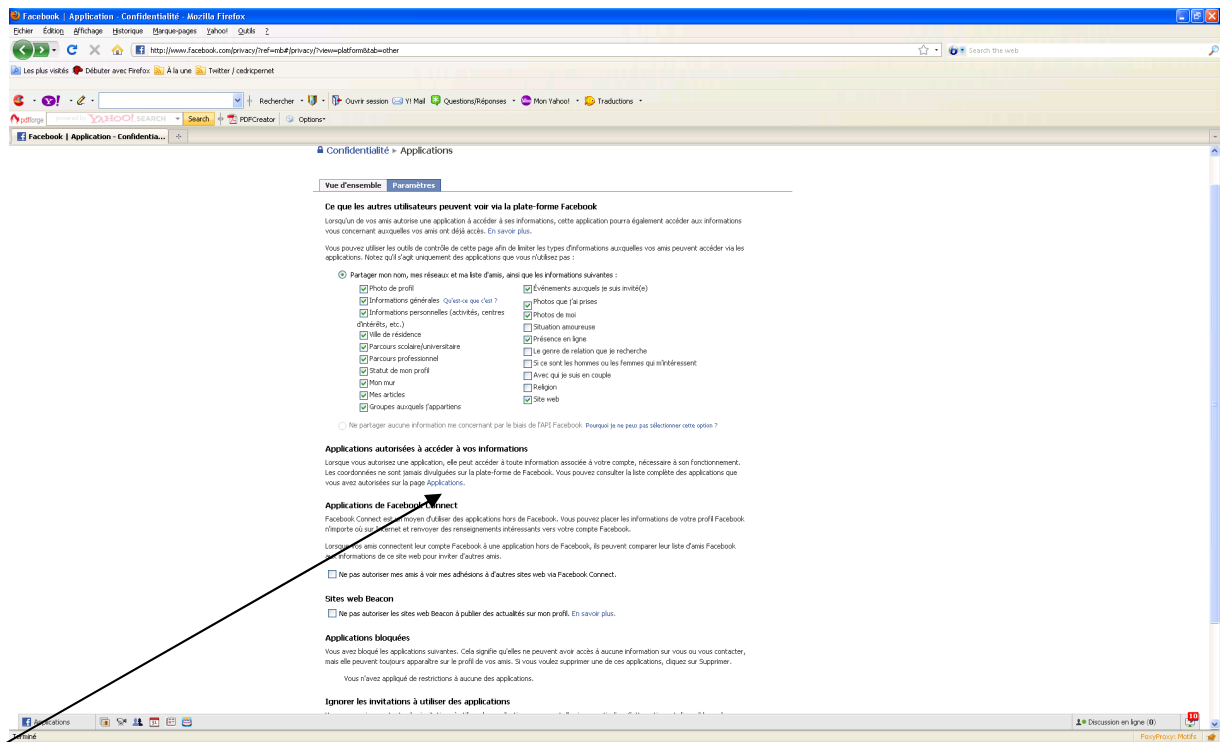
En allant sur une des pages d'une application, celle-ci peut, sans même que vous ne vous en rendiez compte, récupérer ni plus ni moins que l'ensemble des données – date de naissance, statut relationnel, intérêts, opinions politiques, etc. - que vous avez renseigné de votre plein gré sur votre profil, ainsi que vos événements, groupes, etc. Vous pouvez bien sûr avoir choisi de publier ces informations en connaissance de cause...seulement, cela n'engage pas que vous ! En effet, lorsque vous passerez sur une application, l'auteur de l'application pourra aussi accéder aux informations, événements, groupes, etc. de vos amis et les récupérer.

Recommandation Action Innocence : N'autorisez que « Savoir qui je suis et accéder à mes informations » et « Ajouter une boîte dans mon profil » et surtout n'installez qu'un nombre minimum d'applications.

Récemment, dans le cadre d'une émission télévisée, une récente expérimentation de la BBC a mis en lumière que, via une application sur Facebook, il est possible, non seulement, d'accéder aux données personnelles des membres de cette plateforme, mais aussi de les récupérer. Et contrairement, à ce qu'on pourrait penser, cette application n'a pas besoin d'un haut degré de sophistication en matière de technologie, puisque selon la BBC, « n'importe quelle personne avec des connaissances de base en programmation » pourrait développer une petite application capable d'utiliser et de récupérer les données personnelles des utilisateurs. Par exemple, celle de l'expérience de la BBC a été réalisée en moins de

trois heures. Cette dernière a pu absorber, non seulement, les informations des membres qui ont téléchargé le programme, mais aussi, celles de leurs amis (sans même qu'ils ne puissent s'en rendre compte). Bien que Facebook ait répliqué, arguant qu'il « disposait d'une technologie sophistiquée et d'une équipe spécialisée pour s'attaquer aux activités non autorisées des applications » et qu'il demandait aux créateurs d'applications de se conformer à « des conditions d'utilisation » qui leur interdisent notamment de recueillir les coordonnées des utilisateurs, la prudence est de mise.

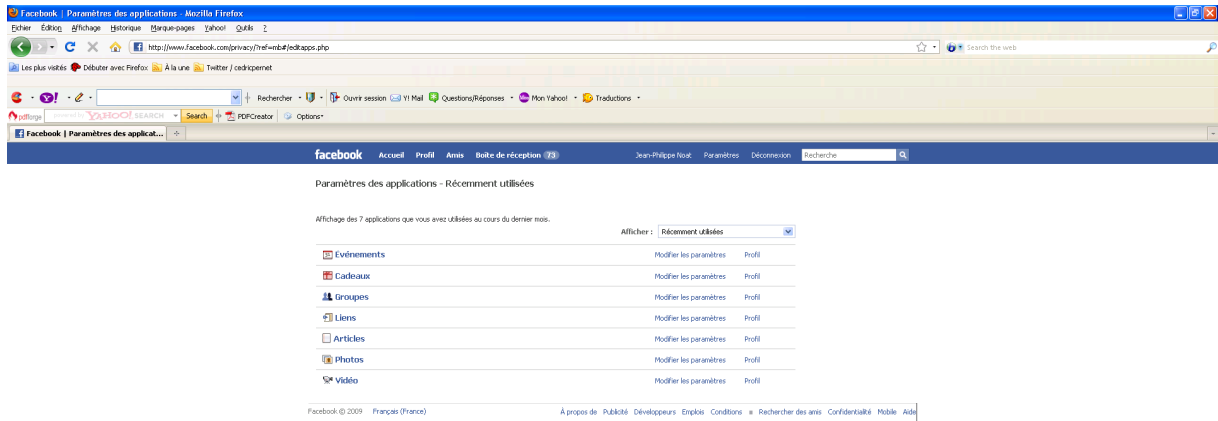
Chaque application peut-être configurée de manière approfondie :



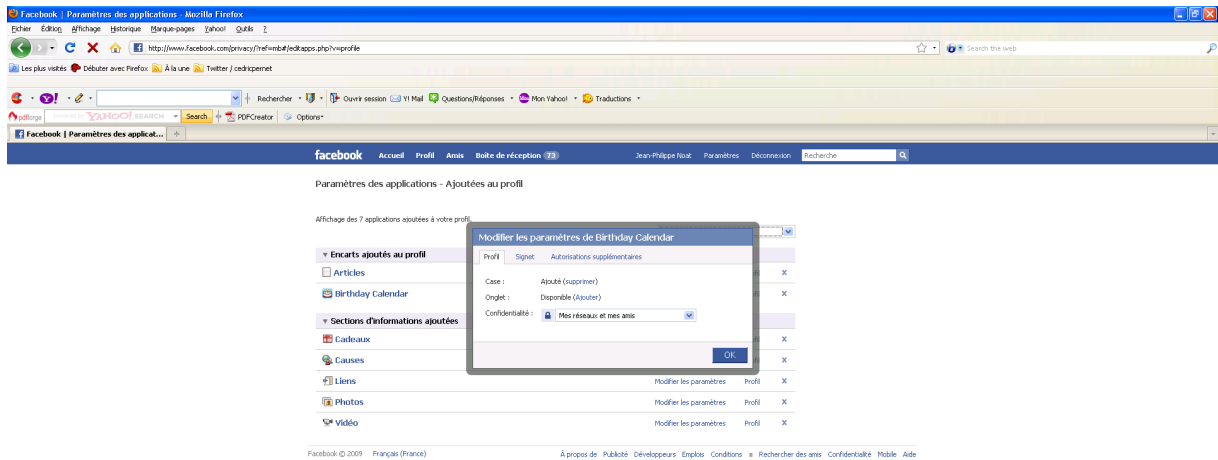
Dans cette partie là on peut d'ores et déjà détailler les informations accessibles aux amis et plus généralement aux réseaux auxquels on appartient.

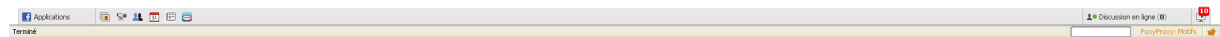
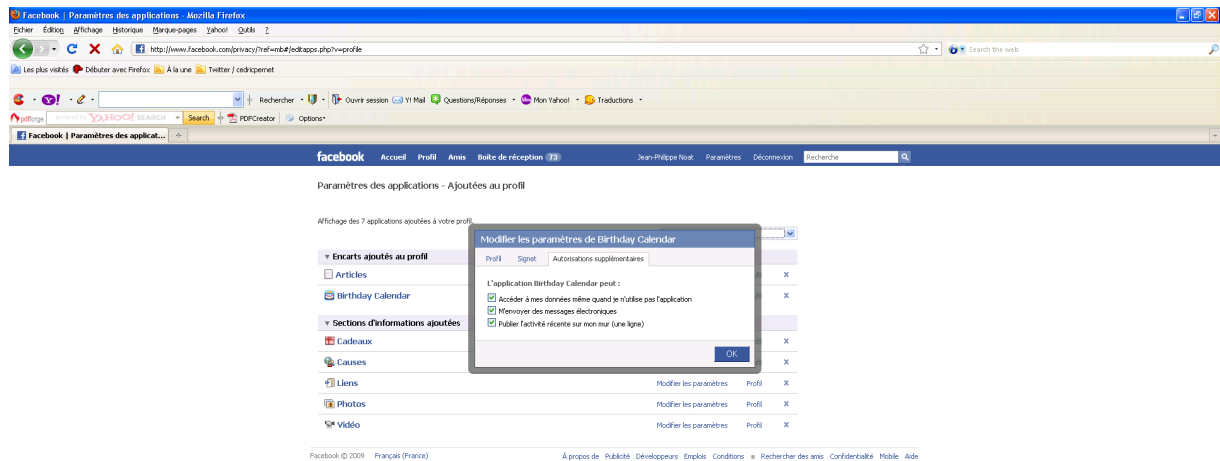
Des informations très personnelles (situation amoureuse, religion,...) existent et il est conseillé de les désactiver (ce qui n'est pas le cas par défaut).

Un lien permet d'accéder plus finement aux applications installées et autorisées :



On accède alors à l'ensemble des applications visibles et installées sur le profil. Chaque application peut ensuite être personnalisée en cliquant sur « Modifier les paramètres ».





Comme on peut le voir sur cette application « standard » de Facebook. Par défaut l'application peut accéder à mes données même quand je ne l'utilise pas. Elle peut m'envoyer des messages électroniques et écrire sur mon mur.

Il est donc important par le biais de ces fonctionnalités de supprimer les applications dont on ne se sert pas et de contrôler au mieux les applications dont on se sert.

A savoir : La grande majorité des applications telles que Groupes, Événements, Funwall, Super Wall, TopFriends, Movies, Are you interested ?, Vampires et bien d'autres sont paramétrées (donc visibles) par défaut sur « mes réseaux et mes amis ». Par conséquent, même si vous avez paramétré l'option Profil du module Profil sur « Seulement mes amis », si vous répondez à un message ou un poke d'un inconnu qui aurait adhéré à votre réseau (qu'il est impossible de masquer), celui-ci pourra voir vos FunWall, Super Wall, Top Friends, etc.

🔒 Confidentialité ▶ Articles

Qui peut voir vos Articles?

🔒 Qui peut voir cela ?
Seulement mes amis

Commentaires

- Tous ceux qui peuvent voir mes articles peuvent publier des commentaires
- Seuls mes amis peuvent publier des commentaires
- Désactiver les commentaires

Publication

- Tous ceux qui peuvent voir mes articles peuvent s'y inscrire
- Personne ne peut s'abonner

Enregistrer Annuler

Pour l'application Articles, cette option permet alors de choisir s'il est possible de laisser des commentaires ou pas, qui est autorisé à le faire, et s'il est possible de s'y abonner.

Pour l'application Photos, cette option permet de définir qui peut voir chacun de vos albums photos. Pour les albums photos que vous souhaitez montrer qu'à quelques « amis » : Personnaliser > Certains Amis (tapez les noms ou une liste) + Aucun de mes réseaux (à ne surtout pas oublier!)

...et pour les autres : sélectionnez « Seulement mes amis »

Confidentialité ► Photos

Contrôlez qui peut voir chacun de vos albums photos.



The screenshot shows two photo albums with their privacy settings. The first album, 'Animaux', has a photo of a parrot and its privacy is set to 'Seulement mes amis'. The second album, 'Paysages', has a photo of a blue sky with white clouds and its privacy is also set to 'Seulement mes amis'. A dropdown menu is open for the 'Paysages' album, showing options: 'Tout le monde', 'Mes réseaux et mes amis', 'Ami(e)s d'ami(e)s', 'Seulement mes amis', and 'Personnaliser...'. Below the dropdown are two buttons: 'Enregistrer les paramètres' and 'Annuler'.

Partager mon nom, mes réseaux et ma liste d'amis, ainsi que les informations suivantes :

- | | |
|---|--|
| <input type="checkbox"/> Photo du profil | <input type="checkbox"/> Événements auxquels vous êtes invité(e) |
| <input type="checkbox"/> Info de base Qu'est-ce que c'est ? | <input type="checkbox"/> Photos prises par vous |
| <input type="checkbox"/> Infos personnelles (activités, centres d'intérêts, etc.) | <input type="checkbox"/> Photos de vous |
| <input type="checkbox"/> Ville actuelle | <input type="checkbox"/> Situation familiale |
| <input type="checkbox"/> Cursus scolaire | <input type="checkbox"/> Présence en ligne |
| <input type="checkbox"/> Historique professionnel | <input type="checkbox"/> Le type de relation que vous recherchez |
| <input type="checkbox"/> Statut du profil | <input type="checkbox"/> Votre orientation sexuelle |
| <input type="checkbox"/> Mur | <input type="checkbox"/> Avec qui vous êtes en couple |
| <input type="checkbox"/> Articles | <input type="checkbox"/> Religion |
| <input type="checkbox"/> Vos groupes | |

Ne partager aucune information me concernant par le biais de l'API Facebook [Pourquoi ne puis-je pas sélectionner cette option ?](#)

Pour les applications pour lesquelles vous n'avez ni autorisé ni explicitement réduit les accès, vous pouvez choisir les informations qui seront mises à disposition de vos amis ainsi que des utilisateurs qui pouvaient déjà voir vos informations sur Facebook.

Recommandation Action Innocence : Décochez toutes les cases

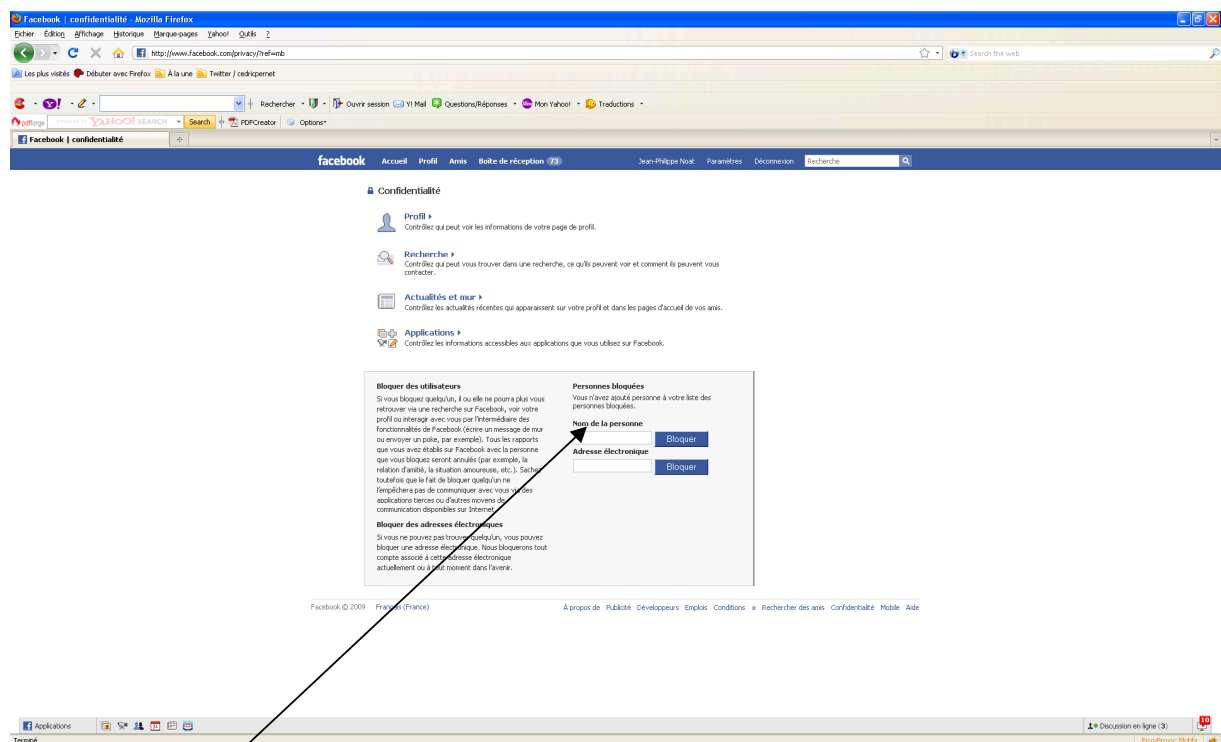


« Vous publiez sur ce site des informations (...) à vos risques et périls (extrait de la politique de confidentialité de Facebook) : le message ne peut être plus clair...alors soyez prudent et réfléchissez à deux fois avant de publier une information personnelle et d'accepter de nouveaux « amis » ! Les utilisateurs de Facebook sont prévenus : « Même si nous vous permettons de définir des options de confidentialité visant à limiter l'accès à vos données, soyez conscient qu'il n'existe aucun système de sécurité infailible. (...) Nous ne pouvons donc en aucun cas garantir que le contenu que vous publiez sur ce site ne sera pas vu par des personnes non autorisées ». Ce sera le mot de la fin sur cette partie !

Comment bloquer des « amis » ou des inconnus indésirables ?

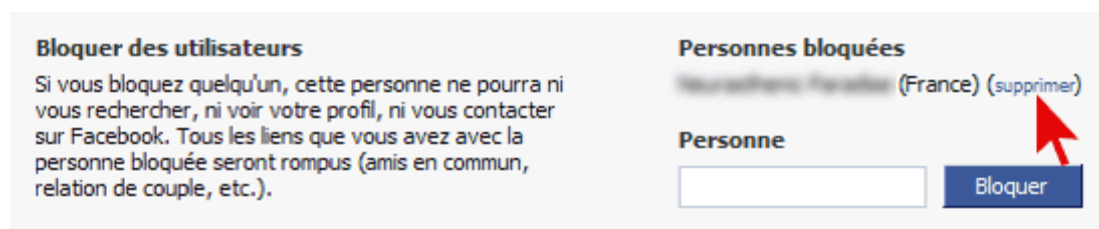
Que ce soit un « ami » que vous avez accepté un peu trop rapidement ou un inconnu qui vous bombarde de messages indécents, il vous est toujours possible de « blacklister » une personne c'est-à-dire de faire en sorte qu'elle ne puisse plus/pas voir votre profil, ni même vous contacter.

Pour cela, il suffit simplement de taper ses nom et prénom dans le champ + Bloquer. Remarque : cela marche aussi dans le champ « adresse électronique ».



A savoir : L'indésirable pourra toujours voir votre profil public c'est-à-dire votre photo de profil et cinq de vos amis en faisant une recherche sur un moteur de recherche tel que Yahoo ou Google si vous n'avez pas décoché l'option Profil Public/ Public Search Listing du module Recherche / Search (voir le module Recherche / Search).

Si vous changez d'avis concernant cette personne, vous pourrez toujours la « débloquer » en cliquant sur Supprimer.



Comment créer une liste limitée d'amis « proches » (exemple pour les albums photos)

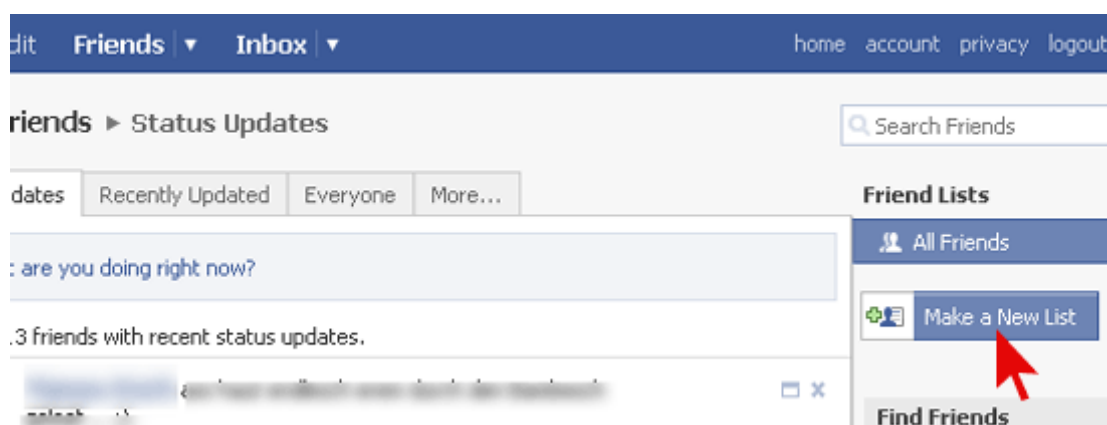
Un grand nombre d'options Facebook sont personnalisables.

- Personnaliser > Seulement mes amis + Aucun de mes réseaux > Excepté ces personnes ou une liste
- Personnaliser > Certains amis + Aucun de mes réseaux > Tapez le nom des personnes ou une liste

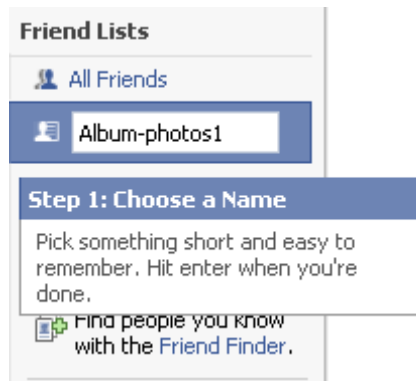
En créant une liste de personnes que nous nommerons « liste limitée » et en leur attribuant certains privilèges vous pourrez décider des informations personnelles, album photos, groupes, articles consultables par telle ou telle personne.

Exemple : création d'une « liste limitée » autorisés à voir l'album photos.

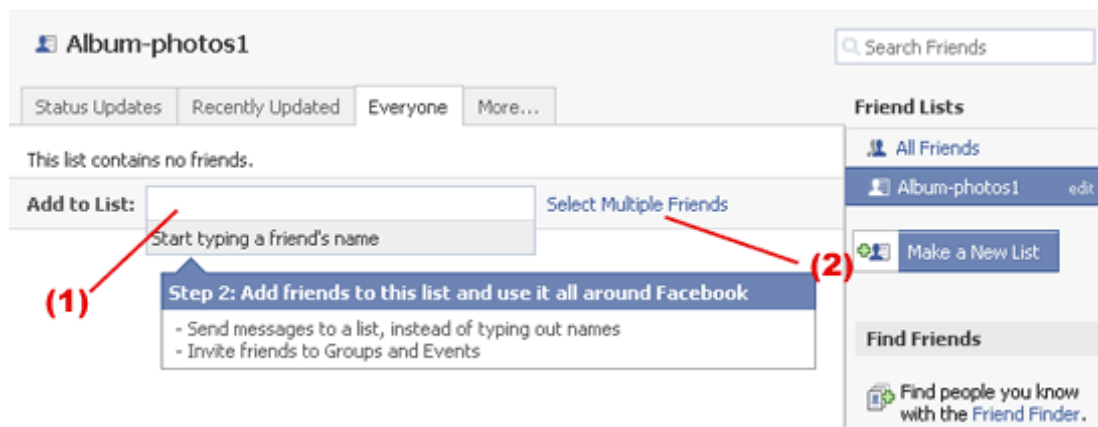
Cliquer sur « Amis » puis « créer une nouvelle liste » ou « Make a New List »



Saisir le nom de la liste (Ex Album-photos1)



Tapez le nom des personnes de la liste (1) ou Cliquez sur Select Multiple Friends (2).



Sélectionnez les amis + Save List.

Votre liste est créée. Ne reste qu'à l'utiliser par exemple pour définir qui peut avoir accès à vos albums photos.

Edit My Applications

Use this page to control which applications appear on your profile, application menu, or News Feed. You can change your preferences at any time.

[Browse more](#)

Edit Profile Box Privacy

Who Can See This?

Friends

- Friends of Friends
My friends and their friends can see this. disabled
- Only Friends
Only friends can see this. disabled
- Some Friends
Choose specific friends who can see this. disabled

Search:

Networks

None of My Networks

Except These People

Okay Cancel

Conclusion

Cette version a été faite avec Facebook en novembre 2009. Nous espérons qu'elle vous aura appris à utiliser au mieux cet outil qui a certes de nombreux avantages mais également de nombreux dangers. La seule personne capable de les réduire c'est vous.