

LE GUIDE DU BON SENS NUMÉRIQUE



20 conseils /

indispensables pour faire preuve
de Bon Sens Numérique **sur les médias
et les réseaux sociaux.**



AXA
prévention
La prévention responsable

SOMMAIRE

Éditorial	3
1 4 notions incontournables pour comprendre le Bon Sens Numérique	4
2 Qui est responsable de la protection de votre vie privée sur Internet ?	6
3 Comment faire face aux délinquants numériques ?	10
4 Comment protéger votre identité et votre réputation sur Internet ?	14
5 Comment gérer au mieux les interactions entre marque personnelle et marque d'entreprise ?	18
Conclusion	22
Glossaire	23
Bibliographie	23

Prévenir et gérer les risques numériques

par **Éric Lemaire**

Président de l'association AXA Prévention



Réinventer notre métier d'assureur, c'est aussi réinventer notre manière de réduire les risques et d'innover en permanence dans la façon de sensibiliser nos différents publics.

AXA Prévention, association loi 1901, agit ainsi depuis près de **30 ans pour protéger le grand public, les clients et les collaborateurs d'AXA France** sur les grands risques du quotidien : risque routier, santé, accidents de la vie courante...

Les médias et les réseaux sociaux connaissent un développement formidable : ils offrent chaque jour de nouvelles perspectives de communication et d'interactivité entre les personnes, que ce soit dans le cadre d'une utilisation professionnelle ou privée. Sur Internet, l'information est instantanée, démultipliée presque à l'infini.

Notre vie s'enrichit et se prolonge d'une vie numérique. Elle démarre dès l'instant où nous

sommes connectés à Internet, devant notre écran d'ordinateur, notre Smartphone ou notre tablette.

Dans notre vie numérique, nous publions des contenus, nous entretenons des liens virtuels, nous partageons, discutons, commentons... Nous y dévoilons, par petits morceaux, notre vie personnelle comme professionnelle. Or, **chacune de nos actions va laisser des traces numériques, qui peuvent avoir des conséquences, aujourd'hui ou demain, positives ou négatives, dans notre vie « réelle ».**

Il manquait un « code de la route numérique » pour accompagner les internautes dans la compréhension des usages. Ce Guide du Bon Sens Numérique est un premier pas **pour répondre à ce besoin, permettre à tous d'acquérir des comportements responsables sur Internet, et ainsi profiter des espaces d'échange et de partage d'information en toute sécurité.**

Avant de lire...

Les **20 conseils de Bon Sens Numérique** présentés dans ce guide sont le fruit des contributions postées sur une « **plateforme d'intelligence collective** » par les collaborateurs d'AXA France. Vous retrouverez dans les pages qui suivent certaines de leurs contributions. Pour vous aider, le glossaire page 23 propose une brève définition des termes liés au **Web 2.0**.

4 NOTIONS INCONTOURNABLES

pour comprendre le Bon Sens Numérique



Notion n°1

Web 1.0 et Web 2.0

Le **Web 1.0** est principalement composé des sites Web d'information, des sites d'organisations et des sites d'entreprises qui diffusent des contenus comme celui d'AXA France : www.axafrance.fr. **Dans le Web 1.0, une personne publie une information pour plusieurs personnes.**

Le **Web 2.0** est composé de **médias sociaux et de réseaux sociaux**. **Dans le Web 2.0, tout le monde peut publier une information sur laquelle chacun peut réagir.**

– Les **médias sociaux** permettent de produire du contenu : blogosphère, twittosphère, forums, journaux participatifs type Agoravox, présentation type PowerPoint (www.slideshare.net), **wikis**...

– Les **réseaux sociaux** physiques (associations, clubs...) ou virtuels (**LinkedIn**, **Facebook**...) connectent des individus.

Notion n°2

Vie physique et vie numérique

Pour désigner l'ensemble des actions que vous entreprenez dans l'espace virtuel qu'est Internet, nous parlons de « vie numérique ». Celle-ci se traduit par les profils que vous identifiez sur les **réseaux sociaux** et le contenu que vous publiez (texte, photo, film) sur les **médias sociaux**.

Notion n°3

Identité et réputation numérique

Votre identité est ce que vous déclarez sur vous-même. Vous avez une « identité sociale » (familiale ou récréative) et une « identité professionnelle ». Lorsque vous publiez votre CV sur les réseaux sociaux comme **LinkedIn**, **votre identité devient numérique.**

Votre réputation est ce que les autres pensent de vous. Vous avez une « réputation sociale » et une « réputation professionnelle ». Lorsque votre entourage professionnel donne son opinion sur vos compétences à travers des recommandations sur les réseaux sociaux ou sur les médias sociaux, **votre réputation devient numérique.**

Votre identité et votre réputation se construisent désormais sur le net. **Pour les découvrir, il faut se « googler »,** c'est-à-dire taper votre prénom et votre nom entre guillemets dans un moteur de recherche comme **Google** (le leader) ou Bing.

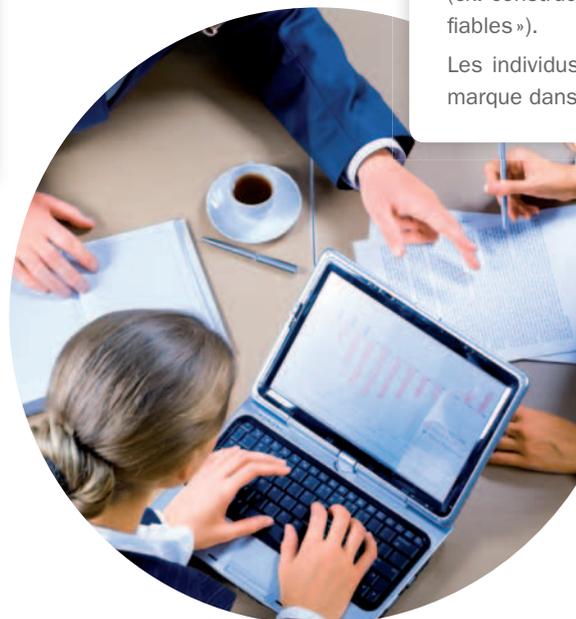
Notion n°4

Marque d'entreprise et marque personnelle

Une marque personnelle est l'addition de **l'identité d'une personne** (ex. responsable marketing) et de **sa réputation** (ex. « un excellent expert du marketing »).

Une marque d'entreprise est l'addition de **l'identité d'une entreprise** (ex. constructeur automobile) et de **sa réputation** (ex. « des voitures fiables »).

Les individus comme les entreprises doivent gérer et protéger leur marque dans le monde physique et numérique.



Entendez-vous pour la première fois cette notion de « marque personnelle » ?

Des expressions du langage courant associent déjà un individu à une marque :

- > Il faut se **démarquer**
- > Avoir une bonne image de **marque**
- > Imprimer sa **marque** dans un projet
- > **Marquer** les esprits
- > C'est sa **marque** de fabrication

QUI EST RESPONSABLE de la protection de votre vie privée sur Internet ?

Internet est par nature **un espace public sur lequel des sites Web vous offrent des espaces privés** où vous pouvez partager des contenus avec d'autres personnes. On parle alors d'espaces partagés. Le plus utilisé est le réseau social **Facebook** mais il en existe d'autres. Pour les nommer, nous utiliserons le terme « **réseaux sociaux** ».

Ces espaces privés ou partagés sont publics. Il suffit d'un clic pour que votre entourage copie puis colle le texte ou l'image publié sur votre mur Facebook et le duplique sur un autre « espace privé » ou simplement sur un forum public ou un blog.

Voici un exemple avec l'image ci-dessous, clic droit sur l'image, menu « copier l'image » ou « enregistrer l'image sous... ». C'est aussi simple qu'un copier/coller dans un logiciel de traitement de texte.

Vos amis peuvent aussi tout simplement rendre publics vos contenus en montrant leur écran aux personnes dans la même pièce. Aucune compétence technique n'est nécessaire !

En résumé, **protéger sa vie privée sur Internet est une responsabilité individuelle et non celle des réseaux sociaux** :

- parce que les réseaux sociaux vont continuer de modifier fréquemment leurs conditions générales d'utilisation,
- parce que votre compte peut être piraté (vol de votre identifiant et mot de passe),
- parce que les bugs informatiques existeront toujours et pourraient donner accès à vos données,
- parce que les réseaux sociaux ont besoin de vos données privées pour commercialiser leurs espaces publicitaires,
- et, comme nous l'avons dit, parce que votre entourage peut dupliquer vos données privées.

Même si vous devenez un expert du paramétrage de la confidentialité sur votre réseau social préféré, vous n'avez aucune garantie que vos informations resteront confidentielles.



Conseil n°1

Public un jour, public toujours

Publiez des informations sur votre vie privée seulement si vous êtes prêt à ce qu'elles deviennent **publiques un jour**. Ce que vous postez sur Internet peut être accessible très longtemps.

Conseil n°2

Anticiper l'avenir

Un contenu peut être sans conséquence aujourd'hui mais nuire à l'image que vous souhaiteriez donner demain. On ne peut pas anticiper sur tout, mais on peut essayer d'y **réf échir une minute avant de cliquer sur sa souris**.

Conseil n°3

Protéger l'intimité de sa vie privée

Vous avez deux vies privées. Il y a votre vie privée dans un **espace public** (restaurant, rue, jardin, boulangerie...) et votre vie privée dans un **espace privé** (votre domicile, votre voiture...) que l'on appelle aussi *l'intimité de votre vie privée*.

Vous vous trouvez dans un restaurant et vous vous apercevez que votre voisin de table écoute discrètement votre discussion. Vous restez à votre table, car ce que vous dites sur **voire vie privée** n'a pas d'importance. Mais comme vous savez que quelqu'un écoute, vous ne parlerez pas de *l'intimité de votre vie privée*.

Quand vous êtes sur les réseaux sociaux, vous êtes à une table de restaurant (c'est votre vie privée dans un espace public). Tout le monde peut vous voir et vous entendre. **Alors, ne faites pas sur les réseaux sociaux ce que vous ne feriez pas dans un restaurant.**



Conseil n°4

Dis-moi qui tu connais, je te dirais qui tu es !

Si votre usage des réseaux sociaux est purement récréatif (non professionnel), connectez-vous uniquement avec **vos vrais amis**. Plus vous limitez le nombre de personnes qui ont accès à vos informations, moins il y a de chance qu'elles deviennent publiques.

Ils ont dit...

“ **Mickael M.** : *Il est important de bien différencier les catégories de personnes que nous fréquentons chaque jour et auxquelles nous ouvrons une porte sur notre vie. Dans le monde physique, nous compartimentons l'accès à notre vie privée. Ainsi nos amis, nos collègues, nos voisins n'auront pas le même niveau d'information. Lorsque l'on a 500 ou 1 000 « amis » sur Facebook, on ne peut pas penser que ce sont tous des amis d'un niveau où l'intimité peut être dévoilée.* ”

Conseil n°5

Faire preuve de Bon Sens Numérique envers les autres

Faire preuve de Bon Sens Numérique, c'est **respecter la vie privée de votre entourage, de vos amis, de votre famille** et se mettre à la place des autres en adaptant votre comportement en fonction des cultures, habitudes, exigences et contraintes des uns et des autres.

Ils ont dit...

“ **Bénédicte D.S.** : *« Pour ma part, je ne poste pas de photos sans l'accord des personnes concernées. Je comprends que certains membres de ma famille ne souhaitent pas être visibles sur les médias sociaux. »* ”

Conseil n°6

Aller voir le « Best of des boulettes numériques » et tenter de ne jamais y figurer

En un clic, votre entourage peut dupliquer du contenu dans un espace public. Et **certaines « amis » sont moins bienveillants que d'autres**. Il existe de nouveaux sites qui affichent publiquement **le pire des publications sur Facebook**. Parmi ces sites, il y a www.stupidbook.fr ou www.zeros-sociaux.fr. Ce sont les internautes qui soumettent les publications à l'insu de leurs auteurs.

Vous avez une vie personnelle et une vie professionnelle, pourquoi pas deux profils ?

C'est une cloison qui sera plus étanche que les options de création de groupes proposées par **Facebook** et **Google +**, **qui ne prennent pas en compte les évolutions de vos relations** : les amis qui deviennent vos ennemis ; votre ami qui devient votre supérieur ; votre collègue qui devient un ami.



Rien ni personne ne vous oblige à publier quoi que ce soit de votre vie privée sur Internet. **C'est votre choix et votre seule responsabilité.**

Protéger sa vie privée et l'accès à ses informations personnelles est important pour **préserver l'intimité de sa vie privée**. Mais, cela l'est davantage lorsqu'il s'agit de **protéger ses biens**. Les voleurs aiment vos données personnelles. Que faites-vous pour les protéger?

COMMENT FAIRE FACE aux délinquants numériques ?



Internet est un outil fantastique pour les délinquants numériques. Certains veulent voler vos biens, d'autres cherchent à usurper votre identité.

Les cambrioleurs vont **évaluer votre patrimoine** à l'aide des photos de votre intérieur que vous rendez publiques sur **Facebook, Flickr** et autres sites de partage de photos. Vous êtes tellement fier de votre nouvelle TV plasma, mobilier, tableau, que vous voulez le partager avec vos « amis ».

Pour **choisir la date du cambriolage**, rien de plus facile. Vous avez annoncé vos dates de vacances plusieurs semaines à l'avance sur votre **mur Facebook** et une fois sur place, vous ne résistez pas à l'envie de publier vos photos sur la plage. Et puis, le jour du départ, vous n'oubliez pas de faire un **tweet** (petit message de 140 caractères sur **Twitter**, sorte de SMS public) pour annoncer que vous êtes au comptoir d'embarquement de l'aéroport.

Enfin, il ne reste plus qu'à **trouver votre adresse** mais vous l'avez publiée sur des profils en ligne ou vous utilisez peut-être **Foursquare**, un service de géolocalisation qui permet d'indiquer votre localisation en temps réel.

L'usurpation d'identité est un délit qui existait bien avant Internet mais qui prend de l'ampleur grâce à toutes les données de votre état civil que vous avez « partagées » avec vos « amis » de manière publique. Le but de l'**usurpation d'identité** est de **faire des faux papiers**, qui vont servir à **obtenir un permis de conduire** par exemple ; mais, le plus souvent, il s'agit de **contracter un prêt à la banque** (c'est l'usurpateur qui encaisse l'argent du prêt, c'est vous qui le remboursez).

Combien coûte l'usurpation d'identité ?

Fin 2009, le Centre de recherche pour l'étude et l'observation des conditions de vie (Credoc) estimait à **210 000 le nombre annuel d'usurpations d'identité en France**. Il révélait aussi que nous sommes plus souvent victimes d'une usurpation d'identité que d'un cambriolage (150 000/an) ou d'un vol de voiture (130 000/an). Le risque d'**usurpation d'identité** est sous-estimé.

74% des cas d'**usurpations d'identité** débouchent sur un délit financier. **Le coût individuel moyen se monterait à 2 229 euros**, cumulant les détournements, le montant des démarches administratives et judiciaires (sondage réalisé par le Credoc auprès de 300 victimes).

Conseil n°7

Ne pas publier son lieu et sa date de naissance

Votre date de naissance est un élément très fort pour vous authentifier. Elle est utile lorsque vous perdez votre mot de passe pour accéder à votre banque en ligne ou lorsque vous effectuez des achats en ligne avec votre carte bleue.

Conseil n°8

Ne jamais publier son adresse postale sur un site Internet public

Ne mettez jamais votre adresse personnelle sur des profils publics. Quelqu'un pourrait ensuite **vous rendre visite à votre domicile** pour vous cambrioler (à la recherche de pièce d'identité, de relevés de compte...), **fouiller votre boîte aux lettres** ou **faire vos poubelles** afin d'obtenir les informations qui lui manque pour **usurper votre identité**. Si vous avez peu d'homonymes et que vous avez publié le nom de la ville dans laquelle vous habitez, il suffit d'aller sur les pages blanches de l'annuaire téléphonique pour trouver votre adresse complète.

En revanche, vous pouvez donner votre adresse sur les sites Web sécurisés comme les sites de e-commerce, banque en ligne, impôts... Vous passez en mode sécurisé lorsque **l'adresse URL commence par https au lieu de http et lorsque vous observez un cadenas fermé en bas à droite de votre écran** (la position peut varier en fonction des navigateurs).

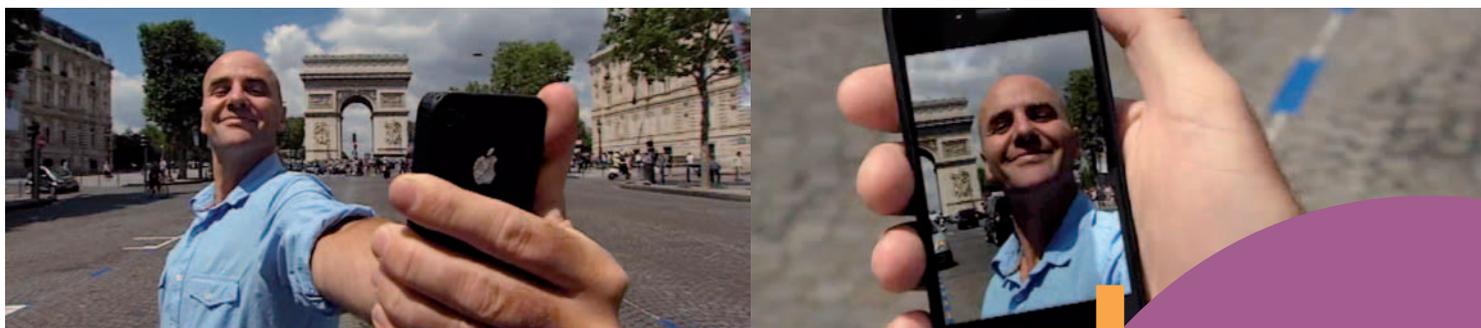
Conseil n°9

Ni vu, ni connu !

N'affichez pas publiquement les dates de vos vacances, de vos déplacements ou vos programmes de week-end.

Ils ont dit...

“ Marie F. : Ce nouveau type de risque donne des idées aux entreprises. En Grande Bretagne, une entreprise de sécurité, Precreate Solutions, propose d'animer les comptes Facebook et Twitter de ses clients en leur absence. Une tactique visant à tromper les potentiels cambrioleurs. ”



Conseil n°10

Eviter de publier des photos de son intérieur

Faites attention à ce que vous publiez en termes de « signes extérieurs de richesse » comme les photos de votre intérieur, de votre nouvelle voiture (belle voiture, beau patrimoine), de votre collection d'art...

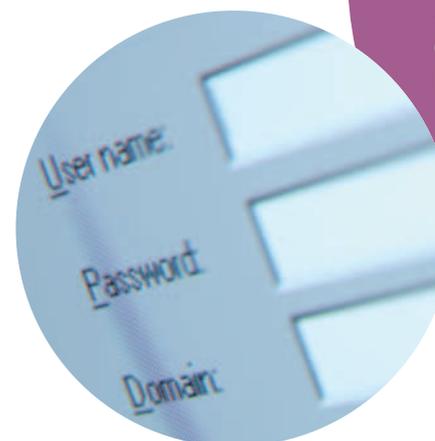
Comment faire quand sa date de naissance est obligatoire pour s'inscrire à un réseau social ?

Même si votre date de naissance peut être utile à vos amis pour ne pas oublier votre anniversaire, elle l'est également aux délinquants numériques et aux annonceurs, qui achètent de la publicité ciblée. Alors, regardez les choses autrement, masquer ou fausser votre date de naissance est le meilleur moyen pour savoir qui sont vos VRAIS amis (ceux qui connaissent votre date d'anniversaire). En bonus, si vous voulez limiter les publicités, indiquez que vous êtes né en 1930. **Peu de chance qu'un annonceur paye pour mettre de la publicité sur votre profil à votre âge !**

“ Dominique M.H. : Il existe un site qui recense les HOAX autrement dit les canulars dont la forme peut être dangereuse et tendre vers de l'arnaque en ligne. L'adresse est www.hoaxbuster.com. Chaque supposée information, scoop ou demande d'aide internationale, aimablement envoyée par mes copains bien intentionnés, est passée par mes soins à la moulinette hoaxbuster. Je vous invite à y faire un tour et survoler les sujets abordés. Regardez bien les dates de création vous allez être surpris, il y a des trucs qui tournent depuis des années... ”

Ils ont dit...

Vos données privées intéressent les délinquants numériques et, en les rendant accessibles, vous leur facilitez le travail. D'autres personnes peuvent s'intéresser à vous sur le net. Ils vont vous « googler » pour savoir ce qui se dit de vous. **Il est donc important de gérer votre marque personnelle et de la protéger.**



COMMENT PROTÉGER votre identité et votre réputation sur Internet ?



La protection de l'identité et de la réputation d'une personne n'est plus une préoccupation réservée aux personnalités publiques, aux stars ou aux célébrités. Cela devient un enjeu pour tous car même si vous ne publiez rien sur vous sur Internet, même si vous n'avez pas d'ordinateur ou pas de connexion Internet, **vos famille, vos amis, votre entourage peuvent publier des contenus (texte ou image) en vous citant nominativement.**

Votre marque personnelle existe sur Internet quoi que vous fassiez et elle devient **une co-construction entre vous et votre entourage.** **Si vous ne vous souciez pas de votre réputation numérique, d'autres le font.** Les médias sociaux sont de plus en plus consultés afin de rechercher des informations sur des personnes. Cette pratique est devenue si courante qu'on emploie l'expression « **googliser ou googler quelqu'un** ».

Ils ont dit...

“ **Ange P. :** Existe-t-il encore des personnes qui pensent qu'Internet n'est que virtuel ? On tend vers une identité numérique de plus en plus proche de la réalité. Cette idée se renforce avec le besoin d'identification favorisé par les réseaux sociaux (photos de profil et autres informations personnelles rattachées). Le pseudo et l'avatar disparaissent au profit d'un véritable patronyme (qui permet de retrouver plus facilement ses amis perdus). Bien sûr, ce changement de comportement affole beaucoup d'entre nous qui deviennent paranoïaques et mettent tout en œuvre pour limiter au possible leur présence sur la toile. Seulement, il faut arrêter de diaboliser le Web et voir les avantages qu'une identité numérique bien conçue peut apporter ! ”

Conseil n°11

Faire une veille sur Internet sur son prénom et son nom

Vous pouvez taper vos prénom et nom entre guillemets sur Google, vous obtiendrez alors les publications contenant cette expression. Pourquoi utiliser des guillemets ? Cela permet d'obtenir les résultats sur la requête « Prénom + Nom » et non ceux qui citent votre prénom ou votre nom uniquement.

Cet exercice vous permettra également de savoir si vous avez des homonymes et de comparer leur visibilité sur Internet par rapport à la vôtre.

Pour davantage de réactivité, nous vous recommandons d'utiliser les alertes Google sur www.google.fr/alerts. Une fois votre compte Google crée, vous pouvez activer gratuitement une ou plusieurs alertes du type « Prénom Nom » ou « Nom Prénom ». Dès que Google indexera une page contenant vos prénom et nom, vous recevrez une alerte par e-mail. Les alertes se limitent à de l'information textuelle. **Si le contenu est négatif, vous pourrez alors mettre en place une stratégie.**

Conseil n°12

Faire disparaître les contenus qui nuisent à sa réputation ou qui sont incohérents avec l'image que l'on souhaite donner

Si le contenu est positif, à vous de le faire savoir en dupliquant ce contenu sur d'autres supports numériques. Mais si le contenu publié ne vous plaît pas, vous allez tenter **d'obtenir sa suppression.**

Un contenu préjudiciable pour vous n'est pas automatiquement un contenu illicite au sens juridique. Ainsi un contenu pourra être jugé illicite s'il relève de :

- la diffamation : le contenu porte atteinte à votre honneur. Ex : Mr X est un ivrogne bien connu comme tel...
- l'injure : le contenu est outrageant, méprisant, injurieux. Ex : X est une petite vermine...
- l'atteinte au droit à l'image : une photo ou une vidéo est publiée en ligne sans votre autorisation. Ex : des photographies privées de vos vacances sont diffusées.
- l'atteinte au droit au respect à la vie privée : le contenu révèle des informations de votre vie privée. Ex : Monsieur X pratique le nudisme l'été.
- l'atteinte aux correspondances privées. Ex : quelqu'un publie, sans votre accord, sur le net un courrier, un email, une conversation téléphonique enregistrée.

Quelqu'un peut-il publier un contenu négatif en vous citant nominativement ?

Tout comme on peut critiquer un sportif, un hôtel ou les produits d'une entreprise, on peut aussi émettre une opinion négative sur vous ou vos actions et la publier sur Internet. La liberté d'expression autorise chacun à exprimer une opinion positive ou négative. Ce qui est interdit, c'est de vous insulter ou de divulguer des faits qui sont faux (diffamation).

Plusieurs voies s'offrent à vous pour obtenir la suppression d'un contenu. Seul le contenu illicite donne accès à la voie judiciaire.

Option 1 La voie amiable

Presque tous les sites Internet vous permettent de supprimer les contenus que vous avez vous-même publiés. Si le contenu qui vous gêne a été publié par une personne de votre entourage, prenez contact avec elle et demandez-lui de le supprimer.

Si vous ne connaissez pas l'identité de l'auteur ou que vous ne souhaitez pas le contacter, regardez dans les mentions légales ou les conditions générales d'utilisation du site les moyens de contacter le Webmaster. En dernier recours, vous pouvez retrouver le nom du propriétaire du nom de domaine et ses coordonnées en utilisant le service www.whois.net.

Quand le contenu n'a rien d'illégal mais qu'il vous crée un préjudice dans votre « cadre de référence », décrivez simplement la nature du préjudice et invitez-le à faire preuve d'empathie. Si le contenu est contraire à la loi, exposez les dispositions légales qui justifient cette demande.

Vous pouvez également exercer votre droit de réponse, qui permet de riposter aux attaques ou de rectifier des informations inexactes. Dans les médias sociaux, vous pouvez publier votre droit de réponse vous-même sur un forum de discussion ou via les commentaires d'un blog par exemple. N'oubliez pas que le droit de réponse doit être exercé dans un délai de trois mois à compter de la date de publication du contenu auquel vous souhaitez répondre. Passé ce délai, le Webmaster pourrait vous le refuser.

Option 2 La voie judiciaire

Si l'option 1 n'aboutit pas, vous pouvez demander le retrait du contenu illicite (diffamation, injure, atteinte au droit à l'image, au droit à la vie privée, aux correspondances privées) par voie judiciaire.

Si vous obtenez finalement la suppression ou la modification du contenu, des traces peuvent malgré tout subsister dans les résultats des moteurs de recherche. Il s'agit du système de cache. La page ou le site n'existe plus mais le lien apparaît toujours dans les résultats du moteur de recherche. Google met à disposition des Webmasters une procédure de désindexation volontaire pour demander la suppression du site ou des pages. Vous pouvez aussi adresser une demande à Google, après identification de votre compte Google, en remplissant le formulaire en ligne : www.google.com/webmasters/tools/removals?pli=1



Comment rendre moins visible une information négative sur les moteurs de recherche ?

95% des internautes qui font une recherche sur Internet ne vont pas au-delà de la 3^e page des résultats soit environ 30 liens. Si l'information négative passe sur la 4^e page, elle continue à exister mais elle devient beaucoup moins visible.

Pour faire disparaître un contenu gênant, il suffit donc parfois de créer du contenu avec vos prénom et nom pour enterrer le contenu négatif. Vous pouvez par exemple, créer un compte sur LinkedIn et sur Twitter, créer des profils en ligne comme <https://profiles.google.com/> ou acheter votre nom de domaine : prenom-nom.com.

Conseil n°13

Les paroles s'envolent, les écrits restent...

Il est plus difficile de comprendre et d'être compris dans le monde virtuel qu'en face à face. Ces difficultés de dialogue sont liées à l'absence des expressions du visage et des intonations de la voix. Il n'y a alors qu'un pas entre incompréhension et agression et cette spirale peut ternir votre réputation. N'écrivez pas sur Internet quelque chose sur une personne que vous ne lui diriez pas en face à face.

Ils ont dit...

“ Pierre T. : Les médias sociaux sont le seul lieu où l'on peut exposer un problème et obtenir l'aide de milliers de personnes, où l'on peut avoir des avis non intéressés sur un produit ou une destination de vacances. Et cela n'intéresse personne d'y voir des propos insultants et choquants. ”

Conseil n°14

Parler à son entourage de Bon Sens Numérique

Votre entourage peut publier des contenus sur vous en vous citant nominativement. Le plus gros risque n'est pas que votre entourage (qui vous aime) publie des choses négatives vous concernant. Le risque, c'est que cela ne corresponde pas à l'image que vous souhaitez donner. Cela va de votre ami qui étale votre vie privée sur son mur Facebook jusqu'à vos enfants publiant des photos de vous sans votre autorisation. Plus le contenu est sensationnel, plus l'information peut se diffuser et se dupliquer mondialement en quelques heures. En donnant ce guide à votre entourage, vous vous rendez également service.

Le site Internet de la Commission nationale de l'informatique et des libertés, plus connue sous le signe CNIL, propose des conseils et des dossiers sur la protection de sa réputation numérique (www.cnil.fr).

Il est important que chacun prenne conscience qu'il a une marque personnelle afin d'être en capacité de la protéger, mais aussi de savoir gérer les interactions entre celle-ci et la marque de son entreprise.

COMMENT GÉRER AU MIEUX

les interactions entre marque personnelle et marque d'entreprise ?



À travers vos profils, vos prises de parole ou celles de votre entourage, il est possible de vous identifier comme salarié d'une entreprise ou d'une organisation et de connaître votre fonction. Cela peut se faire à travers votre profil sur **LinkedIn**, votre biographie sur **Facebook** mais aussi à travers les contenus que vous publiez ou qui sont publiés sur vous.

Un représentant de l'ordre en uniforme dans la rue est à la fois une personne et le représentant d'une institution. Il est regardé en tant que personne (courtoisie, professionnalisme...) mais à travers lui, on apprécie aussi l'institution qu'il

représente. **En tant que salarié, votre marque personnelle est de facto en interaction avec la marque de votre entreprise.**

Les interactions entre votre marque personnelle et la marque de votre entreprise ne sont pas une hypothèse, mais une réalité quotidienne. C'est pourquoi il faut savoir les gérer notamment dans les médias sociaux. Beaucoup de salariés ignorent **les obligations** qui leur incombent lorsqu'ils sont dans les médias sociaux, **alors que ce sont les mêmes que dans le monde physique.**

Conseil n°15

Ne pas divulguer une information sur Internet que l'on ne partagerait pas à l'extérieur de l'entreprise

Tous les salariés doivent respecter la confidentialité des informations qui leur sont confiées par leur employeur ou par les clients de l'entreprise. Les informations sur les produits, les services, la fabrication, les plans marketing et commerciaux, les données financières peuvent avoir un caractère confidentiel et leur divulgation serait préjudiciable pour l'entreprise. Référez-vous au code de déontologie ou au règlement intérieur de votre entreprise pour en savoir plus.

Ils ont dit...

“ Dominique T. : Le fait d'apporter sa contribution sur la Toile ne doit pas nous faire oublier le respect de la déontologie (confidentialité, réserve...). ”

Conseil n°16

Employeurs et salariés ont des engagements réciproques et permanents

Les salariés bénéficient comme tous les citoyens d'un **droit d'expression**. En application du **principe de loyauté**, un salarié ne peut **pas compromettre la réputation de son employeur**. Cette obligation va au-delà des locaux dans lesquels vous travaillez et au-delà de vos horaires de travail. Elle est permanente et s'applique de fait sur Internet.

Conseil n°17

Respecter le droit à l'image et la propriété intellectuelle

Vous ne devez jamais publier des photos de vos collègues de travail, de clients ou de tiers **sans autorisation préalable**. Il en est de même pour l'utilisation des logos ou des marques de votre employeur.

Par ailleurs, **la pratique dans les médias sociaux** en matière de droit d'auteur est de mentionner la source du contenu que vous citez et de mettre le lien vers cette source (que le support soit numérique ou non).

Conseil n°18

S'abstenir de toute attitude inappropriée

Vous ne devez pas dénigrer ou insulter vos concurrents, vos collègues de travail, vos clients, vos partenaires, vos fournisseurs... D'une manière générale, **ne faites pas sur Internet ce que vous ne faites pas au bureau.**

Conseil n°19

Distinguer « parler de son entreprise » et « parler au nom de l'entreprise »

Avant de vous engager dans une discussion sur le net, prenez le temps d'en comprendre le contexte et l'objectif. Vous êtes responsable de la véracité de vos propos.

Lorsque vous vous exprimez, assurez-vous que vos points de vue sont identifiés comme tels et non comme ceux de l'entreprise.

Si vous le jugez utile, vous pouvez préciser dans vos publications (blogs, forums...) ou sur votre biographie que les opinions émises sont les vôtres avec une phrase type : « Les opinions exprimées sur ce site me sont propres et ne représentent pas nécessairement celles de mon entreprise ».

Bien que vous vous exprimiez à titre personnel, il y a une interaction implicite entre votre marque personnelle et celle de votre entreprise.

Comme pour les médias traditionnels, certaines personnes sont autorisées à s'exprimer sur les médias sociaux **au nom de l'entreprise.**

Ils ont dit...

“ Christine A.: Il est important de suivre la conversation dans laquelle nous sommes engagés, de s'assurer d'avoir le temps d'actualiser le contenu et de répondre aux questions et commentaires provoqués par notre publication. ”

Conseil n°20

Entrer dans la conversation, c'est faire des critiques constructives et accepter la critique !

Le Web 2.0 est un espace où tout le monde peut publier du contenu et réagir sur le contenu publié par d'autres, en particulier dans les forums de discussion ou via les commentaires des blogs.

Lorsqu'il y a un désaccord avec votre interlocuteur en face à face, il existe des règles implicites de communication qui vous aident à le gérer d'une manière constructive. Vous allez lui demander de clarifier sa pensée. Votre interlocuteur va reformuler son idée et progressivement chacun va comprendre ce que l'autre a voulu dire. **Sur Internet, ces petits ajustements sont plus difficiles et l'agressivité peut rapidement apparaître.**

À partir du moment où vous êtes identifié comme salarié d'une entreprise, vous êtes considéré en tant que personne et en tant que salarié. **Mettez en avant les faits sur lesquels s'appuient vos opinions.**

Si vous vous sentez agressé, recadrez votre interlocuteur sur la forme pour mieux redémarrer sur le fond. Il est parfois préférable d'ignorer le commentaire.

Avec les médias sociaux, n'importe qui peut publier n'importe quoi en vous citant nominativement. **Cela signifie que vous pouvez être victime de publications injurieuses ou diffamantes du fait de la fonction que vous occupez dans l'entreprise.**

Rappelez-vous que ce que vous publiez aujourd'hui sera un jour public. Ce contenu sera donc accessible par vos clients, vos collègues et par votre hiérarchie.

Dans certaines entreprises, des interlocuteurs sont désignés pour accompagner les salariés dans leur utilisation des médias sociaux tout comme il y a des référents informatiques ou juridiques.

CONCLUSION

Entre ceux qui ont peur et qui n'osent pas et ceux qui confondent maîtrise technique et bon sens, nous sommes dans une phase de transition où tout le monde doit encore apprendre en commettant parfois des erreurs.

Faire preuve de Bon Sens Numérique, c'est savoir gérer les risques, les identifier et les anticiper, mais c'est aussi tirer parti de toutes les opportunités offertes par Internet à travers les médias et les réseaux sociaux.

La prévention des risques numériques, un nouvel engagement pour AXA Prévention.

L'association AXA Prévention mène depuis près de 30 ans des actions de prévention des risques liés à la route, à la santé et aux accidents de la vie courante.

Venez témoigner et échanger sur le Bon Sens Numérique en vous rendant sur notre page Facebook :

 facebook.com/lebonsensnumerique



Merci à toutes celles et à tous ceux qui ont contribué à l'élaboration de ce guide et notamment à Olivier Zara, expert en médias sociaux et réputation numérique.

Directeur de la publication : Eric Lemaire

Responsables Coordination et Elaboration : Valérie Leselbaum, Marie-Christine Fontaine

Conception et réalisation : oxygenemultimedia.fr

Crédits photo : Shutterstock, Hemera Technologies, Comstock Images, Jack Hollingsworth, Jupiterimages, Creatas Images, Stéphane Cohen

Ce document est imprimé sur du papier fabriqué à 100% à base de fibres provenant de forêts gérées de manière durable et équitable ou contrôlées dans une usine certifiée ISO 14001 & EMAS.



Glossaire

Les définitions présentes dans le glossaire sont extraites de l'encyclopédie en ligne **Wikipédia** (www.wikipedia.org). Le principe du wiki est que chaque page est modifiable par les visiteurs afin de permettre l'écriture et l'illustration collaborative des documents numériques qu'il contient. Nous vous invitons donc à vous rendre sur ce site Web pour une définition complète ou actualisée des termes se trouvant ci-dessous.

Avatar

Un avatar est un personnage représentant un utilisateur sur internet et dans les jeux vidéo.

Atteinte à la réputation numérique

Lorsqu'une personne est victime de diffamation, d'injure ou lorsque sa vie privée est divulguée de façon illégale sur un blog, un forum de discussion, un réseau social ou un site web, cela constitue une atteinte à sa réputation numérique. On parle également d'atteinte à sa e-réputation.

Facebook

Facebook est un réseau social permettant à toute personne possédant un compte de créer son profil et d'y publier des informations (photo, vidéo, texte) sur **son mur**. Facebook permet à ses utilisateurs d'entrer des informations personnelles et d'interagir avec d'autres utilisateurs. Lancé en 2004, Facebook comptabilisent plus de 23 millions d'utilisateurs en France (source : septembre 2011, *toutfacebook.fr*).

Flickr

Flickr est un site Web de partage de photos et de vidéos gratuit. C'est un site Web populaire auprès des utilisateurs pour partager leurs photos personnelles, mais aussi des photographes professionnels. En août 2011, le site a franchi la barre des 6 milliards de photos hébergées.

Google

Google est le moteur de recherche le plus utilisé dans le monde pour naviguer sur Internet. En 2011, Google lance son réseau social, **Google+** qui est présenté par de nombreux médias comme un service destiné à concurrencer Facebook.

LinkedIn

LinkedIn est un réseau social professionnel en ligne créé en 2003. En octobre 2011, le site revendique plus de 120 millions de membres issus de 170 secteurs d'activités dans plus de 200 pays et territoires. LinkedIn est un service qui permet de construire et d'agréger son réseau professionnel. Il se définit comme un réseau de connaissances qui facilite le dialogue entre professionnels. Pour ses membres, c'est aussi un outil de gestion de réputation en ligne et de personal branding.

Médias sociaux

Les médias sociaux sont des media qui utilisent des techniques de communication hautement accessibles pour faciliter les interactions sociales. Par le biais de ces moyens de communication sociale, des individus ou des groupes d'individus créent ensemble du contenu Web, l'organisent, l'indexent, le modifient ou font des commentaires et le combinent avec des créations personnelles.

Plate-forme collaborative

Une plate-forme de travail collaboratif est un espace de travail virtuel qui utilise l'intelligence collective dans un esprit de collaboration en ligne. L'objectif du travail collaboratif est de

faciliter et optimiser la communication entre les individus dans le cadre d'un projet ou d'un travail.

Réseaux sociaux

Certains « réseaux sociaux » sur Internet regroupent des amis de la vie réelle. D'autres aident à se créer un cercle d'amis, à trouver des partenaires commerciaux, un emploi ou autres. Il s'agit de services de réseautage social, comme **Facebook**, **Google+**, **Twitter**, **LinkedIn**...

Twitter et Tweets

Twitter est un outil de réseau social et de microblogging qui permet à l'utilisateur d'envoyer gratuitement des messages brefs, appelés **tweets** (« gazouillis » en anglais).

Usurpation d'identité

L'usurpation d'identité est le fait de prendre délibérément l'identité d'une autre personne, généralement dans le but de réaliser des actions frauduleuses commerciales, civiles ou pénales. Le fraudeur peut accéder aux finances de la personne usurpée, peut commettre en son nom un délit, un crime ou accéder à des droits de façon induue. Les conséquences peuvent être lourdes pour les victimes d'usurpation d'identité : pertes financières, poursuites judiciaires, retrait du permis de conduire...

Web 2.0

Le Web 2.0 est une évolution du Web vers plus de simplicité et d'interactivité permettant à chacun de contribuer sous différentes formes. Ainsi, les internautes contribuent à l'échange d'informations et peuvent interagir (partager, échanger, etc.) de façon simple, à la fois avec le contenu et la structure des pages, mais aussi entre eux, créant ainsi notamment le Web social. L'internaute devient, grâce aux outils mis à sa disposition, une personne active sur la toile.

Webmaster

Le Webmaster est la personne responsable d'un site Web et du contenu qu'il présente. C'est lui en général qui décide de la mise en ligne d'un contenu.

Whois

Whois (contraction de l'anglais *who is?*, signifiant « qui est ? ») est un service de recherche fourni par les registres Internet. Il permet d'obtenir des informations sur une adresse IP ou un nom de domaine. Ces informations ont des usages très variés, que ce soit la coordination entre ingénieurs réseaux pour résoudre un problème technique, ou bien la recherche du titulaire d'un nom de domaine par une société ou un particulier qui souhaiterait l'obtenir.

Source : Wikipédia - Avatar, Facebook, Flickr, Google, LinkedIn, médias sociaux, plateforme collaborative, réseaux sociaux, Twitter, Web 2.0, Webmaster, Whois (www.wikipedia.org). Cet article est sous CC-BY-SA (voir le texte de la licence : <http://creativecommons.org/licenses/by-sa/3.0/legalcode>)

Bibliographie

De nombreux ouvrages existent sur le sujet. Voici les principales publications et sites Web qui ont inspiré ce guide :

Texto Alto, *Le guide pratique Facebook : débutant ou expert, un guide pratique pour tous*, Paris, Eyrolles, 2011

Olivier Zara, *Réussir sa carrière grâce au Personal Branding. Gérer son identité et sa réputation professionnelles*, Paris, Eyrolles, 2009

Blog *Identité et réputation numériques* : www.reputation.axiopole.info/

Le site de la Commission Nationale Informatiques et Libertés CNIL : www.cnil.fr

AXA Prévention
313, Terrasses de l'Arche
92727 Nanterre Cedex
Tél. : +33 1 47 74 46 52
Fax : +33 1 47 74 46 62
E-mail : service.axaprevention@axa.fr
www.axaprevention.fr

Association déclarée loi 1^{er} juillet 1901



AXA
prévention
La prévention responsable