

SÉCURITÉ SUR LES RÉSEAUX SOCIAUX



CI-CERT

**CONTACTS:
CÔTE D'IVOIRE - COMPUTER
EMERGENCY RESPONSE TEAM**

Tel : +225 20 34 43 73 / 74

Mail : info@ci-cert.ci

Site web : <http://www.ci-cert.ci/>

Marcory Anoumanbo, Abidjan – Côte d'Ivoire

SOMMAIRE



Introduction	3
Le web collaboratif	4
Historique.....	5
Les réseaux sociaux.....	6
Les dangers liés aux réseaux sociaux.....	7
Les conseils pour se protéger sur les réseaux sociaux.....	10



CÔTE D'IVOIRE - COMPUTER EMERGENCY RESPONSE TEAM

Tel : +225 20 34 43 73 / 74

Mail : info@cicert.ci

Site web : <http://www.cicert.ci/>

Marcory Anoumanbo, Abidjan – Côte d'Ivoire

Introduction

Les réseaux sociaux sont utiles à bien des égards. Ils nous permettent de garder contact avec différentes personnes de notre entourage. Ils nous servent à rester à l'affût de ce qui se passe dans l'actualité. C'est un milieu où l'on peut exprimer et partager nos opinions, nos intérêts, etc. On peut aussi s'en servir pour se divertir.

Les réseaux sociaux sont, à plusieurs niveaux, bien appréciés ! Toutefois, malgré ces avantages, il faut s'assurer de s'en servir de façon sécuritaire afin d'éviter de fâcheuses situations.

Le web collaboratif :

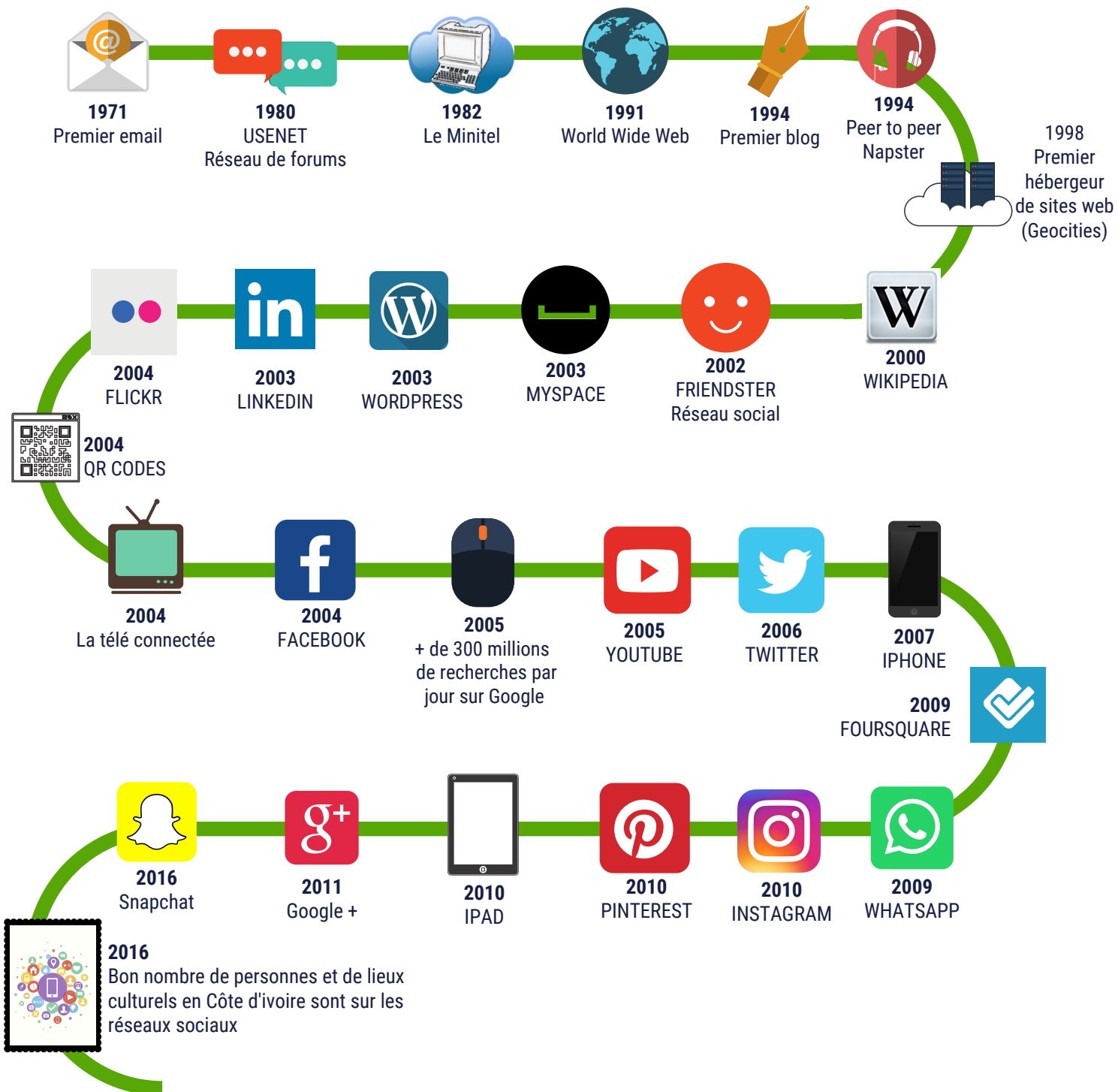
Les réseaux sociaux représentent une avancée du Web vers plus d'interactivité et de facilité d'utilisation. Cela marque l'avènement d'un nouveau rapport aux contenus.

Ainsi l'utilisateur devient dorénavant prescripteur, il veut être actif dans le processus de création.

Auparavant, dans les modes de communication traditionnels, le public était un simple « récepteur ». Aujourd'hui, il peut non seulement réagir aux contenus qui lui sont proposés, mais également créer les siens, transformer ceux des autres et interagir avec eux. Il est devenu un « acteur ». Cette dimension est au cœur des enjeux soulevés par l'utilisation des réseaux sociaux et en fait sa spécificité et sa complexité.

Cette caractéristique est essentielle pour comprendre comment agir sur les réseaux sociaux. Pour les internautes, les réseaux sociaux sont un moyen de personnaliser leurs visites, d'individualiser leurs expériences. Ces plateformes ont acquis au fil des années un statut qui est de l'ordre de celui d'un outil multifonction. L'historique ci-dessous illustre cette évolution.

Historique



Les réseaux sociaux :

Les réseaux sociaux permettent de mettre en relation des individus dont les centres d'intérêts sont communs, en les amenant à coopérer en ligne, voire hors ligne. Ils offrent la possibilité à chacun d'exprimer son opinion, dans une conversation ou un débat, de participer à un projet commun.

Les réseaux sociaux les plus utilisés sont :



FACEBOOK

Créé en 2004, Facebook est le réseau social le plus connu. Il permet essentiellement de garder contact avec son entourage. On y publie des informations (opinions, photos, vidéos, etc.), échange des messages, intègre ou crée des groupes, organise des événements et des rencontres.



TWITTER

Créée en 2006, Twitter est une plateforme de microblogage où les messages ne doivent pas excéder 140 caractères. C'est un média social basé sur l'instantané et c'est l'outil privilégié pour les actualités et les débats du moment.



LINKEDIN

Créé en 2003, LinkedIn est un réseau social professionnel. Il permet d'informer sur votre parcours professionnel, d'établir des relations avec des collègues dans votre domaine, de communiquer avec des employeurs potentiels et d'être approché par des recruteurs.



INSTAGRAM

Créé en 2010 (racheté par Facebook en 2012), Instagram est une application et un service de partage de photos et de vidéos disponibles sur smartphones et tablettes. Les photos et vidéos partagées sur Instagram se caractérisent par une esthétique soignée et inspirante.



PINTEREST

Créé en 2010, Pinterest se présente comme un catalogue d'idées. Il permet de conserver des marque-pages visuels (« épingles ») de vos intérêts dans des catégories (« tableaux »). Les interactions se limitent souvent à s'abonner à un « tableau ».



YOUTUBE

Créé en 2005 (racheté par Google en 2006), YouTube est un site Web d'hébergement de vidéos sur lequel les utilisateurs peuvent envoyer, évaluer, regarder, commenter et partager des vidéos. Les YouTubeurs sont des vidéastes Web amateurs qui partagent leur passion sur la plateforme YouTube.



SNAPCHAT

Créé en 2011, Snapchat est une application mobile de partage de photos et de vidéos. Chaque photo ou vidéo envoyée à un ou plusieurs destinataires est personnalisable et n'est visible que durant une période limitée, à l'issue de laquelle les images s'autodétruisent. Snapchat est largement utilisé par les moins de 25 ans.



WHATSAPP

Fondée en 2009, cette plateforme permet à ces utilisateurs d'envoyer des messages, mais aussi des vidéos, des messages vocaux, des images à leurs amis ou encore à téléphoner. L'application permet également de créer des groupes, ce qui a l'avantage d'avoir des interactions entre plusieurs utilisateurs autour d'une même conversation. Sur WhatsApp, l'utilisateur a un profil, qui lui permet de mettre des informations sur son nom, son statut et sa photo de profil (représentée par une image). Ce profil peut être visualisé par ses contacts.

Les dangers liés aux réseaux sociaux :

La plupart des utilisateurs des réseaux sociaux sont conscients qu'il existe des dangers. Ils sont surtout conscients de ce que l'on appelle les "dangers courants", ce sont les dangers créés par les utilisateurs des réseaux et non les dangers créés par le réseau social en lui-même. Voici certains types de dangers parmi les plus populaires, dont vous devez vous méfier :

CYBERHARCÈLEMENT :

Insultes, moqueries, ridiculisation, menaces, chantage, diffusion de photos compromettantes, etc...

Un clavier peut s'avérer être une arme redoutable. En effet, certains individus se croient anonymes lorsqu'ils écrivent insultent ou menacent et lorsqu'ils présentent des images à des fins illicites. Détrompez-vous, des accusations criminelles peuvent être portées contre les auteurs du cyberharcèlement dès l'âge de 13 ans.

SEXTORSION (CHANTAGE À LA VIDÉO) :

Le chantage à la vidéo se traduit par exemple par le fait qu'une jeune femme se fait aborder sur les réseaux sociaux par un inconnu. Par la suite, une relation plus intime se développe entre les deux internautes. Sous une fausse identité, l'arnaqueur propose à la jeune fille une communication vidéo et finit par la convaincre de s'exhiber alors qu'il enregistre la scène à son insu. L'individu contacte la jeune femme et menace de mettre les images en ligne à moins qu'elle n'accepte de payer une somme d'argent. Si vous êtes victime de sextorsion, il ne faut pas céder au chantage. Ne désactivez pas les comptes qui ont servi à communiquer avec l'arnaqueur. Déposez une plainte à la [Plateforme de Lutte Contre la Cybercriminalité](#) et demandez leur une assistance pour vous aider à retirer les photos compromettantes.

CYBERADDICTION :

La dépendance des réseaux sociaux existe bien tout comme la dépendance à l'alcool ou le tabac. Donc, elle est d'autant plus dangereuse car elle touche les adolescents et les adultes. Elle est également appelée cyberaddiction, usage problématique d'Internet (UPI) ou encore trouble de dépendance à Internet (TDI).

Elle désigne un trouble psychologique entraînant un besoin excessif d'utiliser un réseau social et qui prend la place de la réalité, et de la vie quotidienne. La cyberdépendance se caractérise par l'ensemble des problèmes liés à l'utilisation des réseaux sociaux qui aura un effet négatif et destructeur sur l'utilisateur. De plus, ce phénomène, qui peut être considéré comme une pathologie, s'installe sans qu'on s'en rende compte comme les autres dépendances avec autant de dégâts.

Il existe deux types de symptômes :

Les symptômes psychologiques sont :

- Sentiment de bien-être et d'euphorie lors de l'utilisation des réseaux sociaux ;
- Incapacité à arrêter d'utiliser Internet ;
- Manque de temps pour la famille, les amis ou d'autres loisirs ;
- Problèmes d'assiduité ou de performance au travail ou à l'école ;
- Dépression lorsque la personne est privée d'Internet.

Les symptômes physiques sont :

- yeux secs ;
- maux de tête ;
- maux de dos ;
- repas irréguliers ;
- mauvaise hygiène ;
- insomnies.

DANGER POUR LA VIE PROFESSIONNELLE :

Les réseaux sociaux peuvent constituer un danger dans le milieu professionnel, particulièrement pour les demandeurs d'emploi. En effet certains employeurs, avant d'embaucher une personne, vont rechercher cette personne sur Facebook ou sur Twitter, ces employeurs vont en premier essayer de trouver un profil Facebook pour voir s'il y a des photos compromettantes telles que des photos de soirée ou des photos osées. L'employeur va aussi regarder ses fréquentations, ses statuts ou ses tweets.

LES RÉSEAUX SOCIAUX COMME OUTIL DE RELATIONS PUBLIQUES : UNE MAUVAISE ORGANISATION METTRA EN DANGER L'IMAGE DE L'ORGANISME :

De nombreuses entreprises utilisent les réseaux sociaux pour étendre leur portée et communiquer avec leurs clients. Cependant, les grandes institutions ou entreprises ont souvent un grand nombre de comptes qui doivent être gérés. S'il n'y a pas de responsable des réseaux sociaux qui s'occupe de l'exactitude et de l'actualité du contenu, cela engendre vite une mauvaise impression sur les lecteurs.

Le manque d'organisation de son propre contenu est l'un des dangers des médias sociaux que de nombreuses entreprises sous-estiment. L'espace commentaires ne doit pas non plus être laissé sans modération : une discussion parsemée d'insultes a un effet dissuasif sur les nouveaux lecteurs. Même si les responsables n'interviennent pas en cas de courrier haineux ou de menaces de violence, cela a un effet néfaste sur l'image. Surtout lorsqu'une tempête médiatique survient, les scandales sont inévitables.

Les conseils pour se protéger sur les réseaux sociaux

Les techniques de communication et d'interaction en ligne sont en constante évolution. Ces mesures ont donc été établies pour permettre aux utilisateurs de mieux se protéger sur les réseaux sociaux.

- **VÉRIFIER LES PARAMÈTRES DE CONFIDENTIALITÉ**

Tous les principaux réseaux sociaux ont des règles de confidentialité publiées sur leur site web. Assurez-vous de bien les comprendre mêmes si elles semblent fastidieuses. Certains services offrent la possibilité de restreindre les paramètres de confidentialité, par exemple en vous permettant de partager des photos avec vos amis uniquement et pas avec tout le monde. Faites bon usage de ces paramètres.

- **CHOISISSEZ DES MOTS DE PASSE FORTS**

Choisissez des mots de passe forts, utilisez des mots de passe difficiles à deviner. (Votre date de naissance ou «123456 » ne sont pas des mots de passe forts.) Si possible, le mot de passe doit contenir des lettres et des chiffres, ainsi que des caractères spéciaux.

- **GARDEZ VOTRE MOT DE PASSE SECRET**

Vous ne devriez jamais partager votre mot de passe avec d'autres personnes. Ne perdez pas le contrôle de votre mot de passe. Si vous entrez votre mot de passe, assurez-vous que vous vous trouvez sur le site Web légitime et non sur une page d'escroquerie ou d'hameçonnage ressemblant au site d'origine.

- **SOYEZ PRUDENT**

Vous devez traiter tout ce que vous voyez en ligne avec beaucoup de prudence. Ne croyez pas tout ce que vous lisez qu'il s'agisse de conseil ou de dernières nouvelles. En outre, les personnes sur Internet ne sont pas toujours ce qu'elles prétendent être. La célébrité que vous suivez peut-être tout simplement être un autre fan, et le collaborateur supposé d'un autre bureau pourrait bien être une personne faisant de la reconnaissance sur votre entreprise. Tous ceux qui prétendent être vos amis ne le sont pas tous.

- **ÉVITER DE SE FAIRE IDENTIFIER PAR LA LOCALISATION**

Désactivez les paramètres de localisation et ne partagez jamais l'endroit où vous serez (y compris les sorties en ville et en vacances). Les gens peuvent noter vos habitudes et prédire quand et où vous allez être afin de vous agresser physiquement.

- **NE PAS PARTAGER DES INFORMATIONS PERSONNELLES**

Cela comprend les adresses, l'année de naissance, numéro de téléphone et coordonnées bancaires. Celles-ci peuvent être utilisées par des usurpateurs d'identité.

- **PARTICIPEZ DE MANIÈRE RAISONNABLE**

Réfléchissez toujours à deux fois avant de poster quelque chose. Gardez à l'esprit qu'une fois que vous l'avez posté, même à un groupe d'amis proches, vous n'avez plus le contrôle de sa diffusion. Ces choses peuvent vous porter préjudice plus tard. En outre, évitez de publier des images de nudité, de scènes obscènes et violentes. Soyez respectueux envers les autres et ne postez pas de messages haineux.

- **SOYEZ À JOUR**

Assurez-vous d'avoir à jour votre système d'exploitation, vos logiciels ou applications mobiles, votre navigateur web mais également ses plugins tiers. Certaines des attaques les plus récentes sont très sophistiquées et sont parfois difficiles à détecter par un œil non averti. Utilisez un logiciel de sécurité complet pour vous protéger contre ces menaces.

- Les photos d'enfants ne doivent pas être affichées sans le consentement des parents. Même alors, des photos de nudité, de scènes obscènes et violentes devraient être évitées.



Côte d'Ivoire - Computer Emergency Response Team

Tel : +225 20 34 43 73 / 74

Mail : info@cicert.ci

Site web : <http://www.cicert.ci/>

Marcory Anoumanbo, Abidjan – Côte d'Ivoire