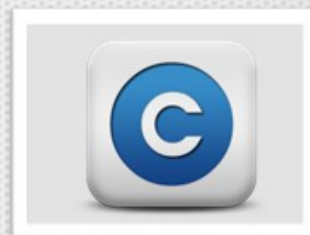
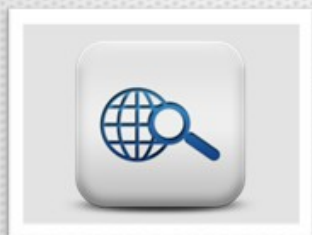


ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE...

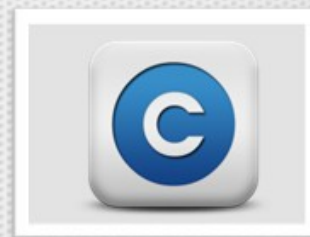
ÇA S'APPREND !



# *KIT DE SURVIE SUR INTERNET*

*Alexandra Lemonnier*  
*Formatrice aux usages d'Internet*

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## PRÉSENTATION

Tout d'abord, merci et félicitations, si vous avez téléchargé ce guide, c'est que vous êtes conscient(e) de l'importance de prendre en charge votre sécurité numérique.

Car il revient à chacun de nous d'apprendre à assurer notre sécurité et à protéger notre vie privée. Personne ne le fera à notre place. Pire : ne pas le faire nous expose à prendre de très sérieux risques.

Ce guide a été conçu de manière à vous permettre de savoir rapidement quels sont les principaux points critiques auxquels vous devez faire attention.

Si vous suivez ces quelques conseils et si vous les transmettez à vos enfants et à votre entourage, vous avez de meilleures chances de ne pas rencontrer les problèmes les plus courants.

Mais attention : les technologies et les usages sur Internet évoluent sans cesse et très rapidement, et les recommandations d'aujourd'hui ne seront peut-être plus suffisantes demain.

C'est pourquoi il est important que vous vous teniez au courant régulièrement et, dans tous les cas, vous devez absolument considérer que **vous êtes le principal acteur de votre sécurité, et de la protection de vos données personnelles et de votre vie privée.**

Internet est l'affaire de tous, au travers des comportements de chacun bien sûr, mais aussi au travers d'une vigilance qui doit s'exercer au niveau des politiques publiques nationales dans le domaine numérique ainsi qu'au niveau des accords et traités internationaux qui auront un impact considérable sur nos vies dans les prochaines décennies.

Puisse ce guide vous aider à avoir un usage d'Internet plus conscient et plus serein, puisse-t-il aussi vous amener à [vouloir comprendre ce qui se passe dans les coulisses d'Internet](#) à notre insu.



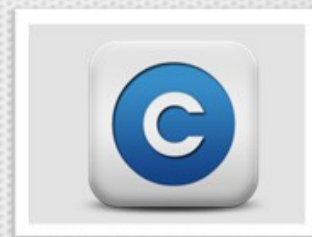
Je vous souhaite une bonne lecture !

Alexandra Lemonnier, formatrice aux usages d'Internet

### ***Droits d'auteur***

*Merci de ne pas modifier ce document qui est protégé au titre des droits d'auteur.  
Vous avez le droit de diffuser ce guide dans votre entourage personnel, mais vous ne pouvez pas  
l'utiliser pour vous créer une liste d'abonnés ni le vendre sous aucune forme que ce soit.  
Merci d'informer autour de vous des possibilités de formation plus poussée.*

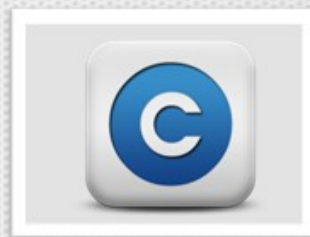
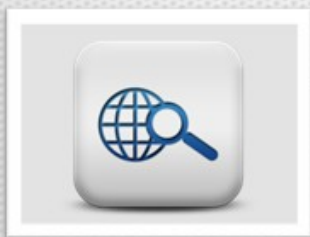
# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## TABLE DES MATIÈRES

INTRODUCTION.....	4
SÉCURITÉ INFORMATIQUE.....	7
LA NAVIGATION SUR INTERNET.....	8
LES MOTEURS DE RECHERCHE.....	9
LES MESSAGERIES.....	10
TÉLÉCHARGEMENTS ET STREAMING.....	11
LES ACHATS EN LIGNE.....	12
LES RÉSEAUX SOCIAUX.....	13
PROTECTION DE LA VIE PRIVÉE.....	14
SAUVEGARDE ET STOCKAGE DES DONNÉES.....	15
COMMUNICATION SUR INTERNET.....	16
MARKETING (ET) INTERNET.....	17
ASPECTS LÉGAUX.....	18
CONCLUSION.....	19
RESSOURCES ET LIENS UTILES.....	20

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## INTRODUCTION

Utiliser Internet aujourd'hui est devenu beaucoup plus complexe qu'il y a ne serait-ce que cinq ans en arrière. Bien sûr, les évolutions technologiques ont rendu pas mal d'opérations plus rapides et plus simples, mais globalement, au vu de l'expérience de dix années d'utilisation d'Internet que j'ai accumulée, je trouve l'usage d'Internet plus difficile et plus risqué qu'à mes débuts.

Pourquoi ? Eh bien tout simplement parce qu'il y a déjà beaucoup plus d'utilisateurs qu'il y a dix ans d'une part, et d'autre part, avec certaines évolutions techniques qui permettent de suivre les internautes à la trace dans tout ce qu'ils font et disent sur Internet, les enjeux économiques ont changé d'échelle et la législation concernant la protection des citoyens n'a pas suivi. Naviguer sur Internet sans se mettre en danger est devenu un vrai parcours du combattant.

De l'espace de partage pacifique et ouvert des origines, on est passé à un terrain miné où les potentialités de profit sont telles, qu'il n'est plus question aujourd'hui d'envisager son usage d'Internet comme quelque chose de complètement innocent.

La mutation est devenue vraiment palpable depuis la démonstration du succès phénoménal des réseaux sociaux. De fait, tous ceux (individus, entreprises) qui ont rapidement compris qu'ils allaient pouvoir tirer un maximum de profit à partir de tout ce que nous faisons et disons sur Internet n'ont pas attendu pour prendre des positions dominantes ou pour mettre leurs armées de programmeurs au travail afin de piéger les pauvres ignorants que nous sommes.

Plusieurs spécialistes du numérique disent simplement que pour ne pas prendre de risques avec Internet, le mieux, c'est de ne pas se connecter du tout... Cette remarque pourrait passer pour cocasse si elle ne témoignait pas d'une réalité qui dépasse très largement la fiction !

Car, quoi que l'on fasse pour sa propre sécurité sur Internet, étant donné que tout appareil qui est connecté est « piratable », que tout fichier numérique peut être falsifié, que l'on ne sait jamais à qui on a affaire sur Internet, les risques pour notre intégrité personnelle sont bien réels.

Ces risques viennent autant d'individus malintentionnés que de multinationales tirant profit des données personnelles que nous livrons naïvement au Web.

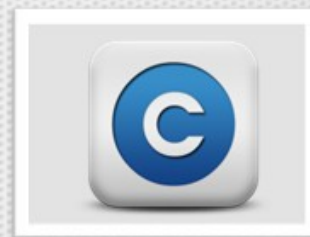
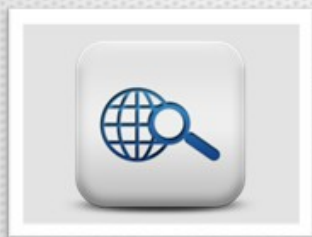
Naturellement, les personnes les plus exposées, et donc le meilleur « gibier » pour tous les prédateurs qui guettent (individus comme entreprises), sont les personnes les moins bien informées. Elles représentent malheureusement la grande majorité des internautes.

Dire qu'il est possible d'éviter tous les pièges serait bien présomptueux, car de nouvelles menaces apparaissent tous les jours et il n'est parfois pas du tout possible de savoir que l'on a par exemple visité un site « infecté » qui a déposé une cochonnerie sur notre ordinateur...



# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE...

## ÇA S'APPREND !



Il n'est pas non plus possible de détecter, sans avoir installé quelques outils particuliers, que toutes nos actions sur Internet et tous les renseignements personnels associés sont tracés puis collectés pour être compilés et vendus à des sociétés dont le seul but est de se rapprocher aussi près que possible de chacun de nous pour nous proposer des produits et des services individualisés et contextualisés, en fonction de nos besoins, de notre situation personnelle, de nos usages, de notre localisation, tout cela en temps réel.

Imaginez aussi ce que pourrait faire un gouvernement un peu trop « curieux » de la vie des citoyens avec toutes ces données... sans parler des banques, des assurances... Dire que l'on n'a rien à cacher n'est pas un argument. Nos libertés fondamentales sont probablement notre bien le plus précieux, nous devons nous assurer qu'elles sont bien garanties. Et pour cela, il nous faut apprendre à nous protéger.

Comprendre quels sont les comportements « à risque » et apprendre ce qui se passe dans les coulisses d'Internet donne de meilleures chances de garantir notre sécurité et permet en tout cas d'éviter les pièges les plus courants. S'il n'est pas possible d'éviter totalement toute menace, il est tout à fait possible de limiter les risques au minimum.

La quantité de savoirs à appréhender pour exercer une forme « d'hygiène numérique » visant à se protéger au mieux est tout à fait considérable et il n'est pas question dans ce guide de délivrer tous ces savoirs, car cela nécessite des développements et des explications beaucoup plus poussés, ce que j'ai fait dans le cadre de la formation que j'ai dispensée à des professionnels de l'animation multimédia et de l'Éducation nationale et que j'ai formalisée à l'intérieur d'une [plateforme en ligne](#).

Mais vous trouverez dans les chapitres suivants des recommandations simples et des outils pratiques et faciles à utiliser qui devraient déjà vous permettre d'avoir un usage d'Internet moins risqué. Le but n'est pas ici d'atteindre l'exhaustivité (ce n'est tout simplement pas possible en aussi peu de temps), mais de pouvoir toucher, par une diffusion gratuite, le plus grand nombre de personnes possible.

Le but n'est pas non plus de fournir une protection clés en main pour savoir installer les outils que je recommande ou configurer ses comptes de réseaux sociaux, car les usages et les compétences de chacun sont trop variés pour qu'une seule et même approche puisse convenir à tout le monde.

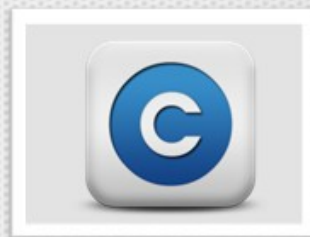
Après avoir parcouru ce guide, vous devriez déjà percevoir la nécessité de changer certaines de vos habitudes de navigation si votre sécurité (et celle de vos enfants) et la protection de votre vie privée sont importantes pour vous. À partir de là, vous pourrez commencer à mettre en œuvre certaines choses par vous-même ou vous référer à [d'autres possibilités d'assistance et de formation](#) si vous préférez être accompagné(e).

Peut-être aussi qu'à la suite de cette lecture, vous éprouverez le besoin de comprendre pourquoi je fais ces recommandations, et quels sont les autres outils et ressources bons à connaître.

Car quand on commence à se poser des questions à propos d'Internet et que l'on découvre de quoi nous sommes l'enjeu (nous tous en tant qu'individus), il n'est plus possible de rester dans la passivité face à des personnes ou des entités qui ont les moyens de prendre le pouvoir sur nos vies et ne sont pas prêtes à se priver de l'exercer. Il y a trop d'argent à gagner sur notre dos et les enjeux de pouvoir sont trop importants !

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE...

## ÇA S'APPREND !



Dans tous les cas, n'oubliez jamais que :

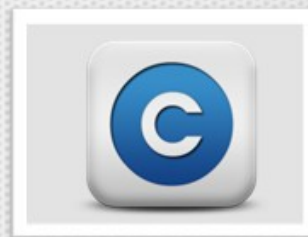
- Internet est avant tout un **espace public partagé**. Comme nos rues et nos routes.
- Nous sommes les premiers responsables de notre sécurité en ligne.
- Tout fichier numérique de tout type peut contenir du code malicieux.
- Tout appareil connecté peut potentiellement être piraté.
- Tout ce qui est en ligne peut potentiellement être piraté.
- Tout ce que nous faisons sur Internet (et hors Internet) peut être tracé.
- Même si certains sites sont plus dangereux que d'autres, il est toujours possible de récupérer un virus ou un programme malveillant sur n'importe quel site.
- Tout ce qui a été mis en ligne peut potentiellement demeurer visible éternellement.
- Les réseaux sociaux peuvent faire ce qu'ils veulent avec nos données et tous les contenus que nous diffusons.
- Toutes les traces que nous laissons sur Internet peuvent être compilées pour déterminer qui nous sommes et ce que nous faisons.
- Tout ce que nous faisons sur Internet peut être utilisé contre nous, y compris par des personnes qui sont nos amis aujourd'hui.
- N'importe qui peut se faire passer pour n'importe qui et dire n'importe quoi.
- N'importe qui peut faire n'importe quoi avec n'importe quel fichier.
- La législation concernant les données personnelles varie d'un pays à l'autre : par exemple, ce qui est vrai pour nous ne l'est pas forcément aux États-Unis...

En gardant ces principes à l'esprit, cela vous mettra déjà dans de bonnes dispositions de prudence élémentaire. Parmi les recommandations que je donne dans ce guide, beaucoup relèvent du simple bon sens et il est possible que vous les appliquiez déjà, par instinct de conservation. Il est possible aussi que vous connaissiez déjà certaines de ces recommandations, ce qui ne fait que confirmer leur validité.

Mais je suis convaincue que dans certains domaines, vous allez découvrir des choses. C'est tout l'intérêt de ma démarche : mettre en relation des thématiques qui ne sont pas reliées habituellement pour vous permettre d'avoir une vision globale de ce qui se joue sur Internet.

Maintenant, voyons thème par thème les quelques recommandations qu'il est bon d'observer.

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## SÉCURITÉ INFORMATIQUE



### À FAIRE

- Maintenez votre matériel informatique (quel qu'il soit) **toujours à jour**.
- Sur Windows, il est indispensable d'installer un antivirus (et un pare-feu de meilleure qualité que celui d'origine), par exemple : [Kaspersky Lab](#), [Bitdefender](#), [Avast](#).
- Mettez à jour votre antivirus **tous les jours**.
- Maintenez [Adobe Reader](#), [QuickTime](#) et [Real Player](#) toujours à jour si vous les utilisez.
- Sur Windows, installez [Spybot Search and Destroy](#) et utilisez [AdwCleaner](#) pour supprimer les programmes-espions ou parasites.
- Chaque fois que vous installez un logiciel, prenez le temps de vérifier chaque étape de l'installation et **décochez toutes les options d'installation d'autres applications**, ce sont le plus souvent des logiciels-espions.

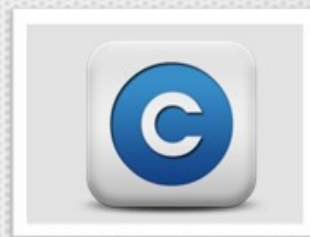
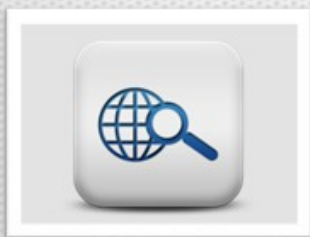


### À NE PAS FAIRE

- Utiliser un antivirus gratuit de marque inconnue est le meilleur moyen d'infecter son ordinateur parfois de façon irrémédiable. Préférez les solutions payantes citées plus haut.
- Évitez de cliquer sur des bannières publicitaires si vous ne pouvez pas vérifier l'adresse de destination en survolant la bannière avec votre souris (l'adresse apparaît en bas de l'écran).
- Évitez de faire des recherches à propos de célébrités en vue qui ont une actualité importante dans les médias.
- Évitez d'installer un logiciel que vous ne connaissez pas ou qui vous a été recommandé par quelqu'un dont vous n'êtes pas sûr(e).



# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## LA NAVIGATION SUR INTERNET



### À FAIRE

- Utilisez de préférence le navigateur [Firefox](#), il respecte la confidentialité de vos données.
- Faites ce qu'il faut pour que votre navigateur soit [toujours à jour](#).
- Prenez le temps de scruter de fond en comble le paramétrage de votre navigateur. Certaines options de traçage sont parfois très bien cachées (notamment dans Chrome) et elles sont activées par défaut.
- Acceptez les mises à jour de [Adobe Flash Player](#) et de [Java](#) lorsqu'elles vous sont proposées.
- Au moment de l'installation de Java, **décochez l'option d'installation de la barre de recherche Ask** (logiciel-espion).
- Activez le contrôle parental chez votre fournisseur d'accès et dans votre antivirus.
- Installez [Ghostery](#) et [Disconnect](#) pour protéger votre navigation.
- Nettoyez [l'historique de votre navigateur](#) et supprimez les cookies régulièrement.
- Utilisez des mots de passe **d'au moins 12 caractères mélangés** (majuscules, minuscules, chiffres et caractères spéciaux) et utilisez un mot de passe différent pour chaque site. Pour le côté pratique et si vous devez créer de nombreux mots de passe, utilisez un [gestionnaire de mots de passe](#).

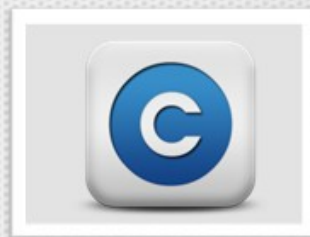
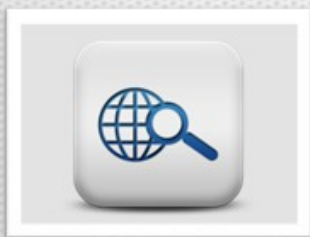


### À NE PAS FAIRE

- Ne cliquez pas sur n'importe quel lien sans en avoir vérifié la destination. Il peut y avoir des redirections risquées entre le lien sur lequel vous cliquez et le site que vous souhaitez visiter.
- Évitez de cliquer sur des liens transmis sur les réseaux sociaux qui ne permettent pas d'identifier le site de destination.
- Ne quittez jamais un poste informatique public ou sur votre lieu de travail sans avoir fermé toutes les applications, tous les sites que vous avez visités, et sans avoir nettoyé l'historique de navigation.



# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## LES MOTEURS DE RECHERCHE



### Pour votre information

Les moteurs de recherche usuels (Google, Bing, etc.) collectent toutes les requêtes effectuées par les internautes et toutes les actions effectuées à partir des résultats de ces requêtes. Ils indexent absolument tout ce qu'ils trouvent sur Internet (textes, images, vidéos, commentaires sur les blogs et les forums, etc.) et sont capables de faire des recoupements pour agréger toutes les données collectées sur n'importe lequel d'entre nous.

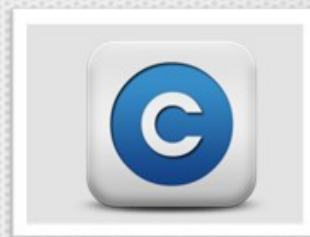
Ne vous méprenez pas sur l'apparente gratuité des outils mis à votre disposition par ces sociétés : rien n'est gratuit dans le sens où elles se « paient » par la collecte de tout ce que nous faisons et disons sur Internet. Les données personnelles sont « l'or noir » du 21<sup>e</sup> siècle et les profits réalisés à partir de ces données sont absolument gigantesques. Pensez aussi que la plupart de ces sociétés sont américaines et que leur livrer nos données sans réfléchir consiste tout simplement à leur livrer les clés de notre économie.



### À FAIRE

- Le moteur de recherche [Startpage](#) permet d'obtenir les résultats fournis par Google tout en rendant vos requêtes anonymes. [DuckDuckGo](#) aussi anonymise vos recherches.
- Supprimez les métadonnées (données associées à chaque fichier numérique créé) des documents que vous publiez sur Internet et qui peuvent contenir de nombreux renseignements, notamment dans les photos par le biais de la localisation. Pour supprimer les métadonnées des photos que vous prenez, voici un logiciel gratuit : [Image MetaData Stripper](#) (pour Windows et Mac).
- Protégez votre vie privée en ne racontant pas votre vie, vos problèmes personnels ou vos problèmes de santé sur les forums, les tchats ou les blogs. Même si vous intervenez sous pseudo, sachez que des techniques de recoupement par comparaison de comportement sont actuellement mises au point pour permettre de profiler une personne, même si celle-ci n'affiche pas clairement son identité sur le Web.

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## LES MESSAGERIES



### À FAIRE

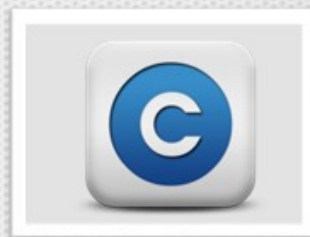
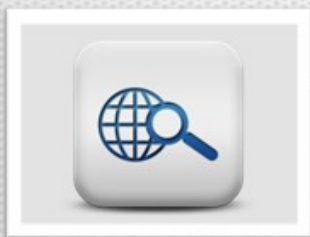
- Utilisez deux messageries : une totalement privée dont vous ne communiquez l'adresse qu'à vos proches, l'autre pour recevoir les messages des sites sur lesquels vous vous êtes inscrit(e).
- Utilisez le logiciel [Thunderbird](#) pour garantir la confidentialité de vos messageries. Autant que possible, évitez d'utiliser Gmail qui scanne tous vos messages pour afficher dans votre messagerie des annonces commerciales ciblées.
- Choisissez un mot de passe fort pour sécuriser l'accès à votre messagerie (12 caractères mélangés).
- Utilisez une [adresse mail temporaire](#) et envoyez des [messages qui s'autodétruisent après avoir été lus](#) par leur destinataire lorsque cela est nécessaire.
- Sachez toujours quels messages vous êtes censé(e) recevoir ou pas et de la part de qui.



### À NE PAS FAIRE

- N'ouvrez jamais un message non attendu, surtout s'il comporte une pièce jointe.
- N'ouvrez jamais une pièce jointe sans savoir de qui elle vient.
- N'ouvrez jamais un message dont l'expéditeur se présente avec son seul prénom.
- Ne remplissez jamais un formulaire lié à un message reçu de la part d'un organisme « officiel » vous demandant de mettre à jour vos coordonnées, notamment celles de votre carte bancaire, mais aussi toute autre donnée personnelle.
- Si vous recevez un message de la part de quelqu'un que vous connaissez et qui prétend être en grande difficulté et avoir besoin d'argent, ne répondez pas, n'envoyez surtout pas d'argent. Appelez votre ami(e) par téléphone si vous avez un doute, mais tout porte à croire qu'on tente de vous escroquer.
- Ne laissez jamais votre adresse mail visible en toutes lettres sur Internet, écrivez-la par exemple de cette manière : adresse [at] fournisseur.fr.

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## TÉLÉCHARGEMENTS ET STREAMING



### À FAIRE

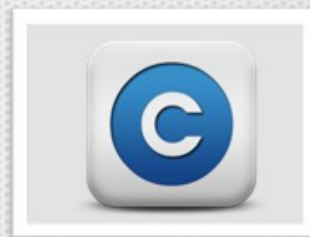
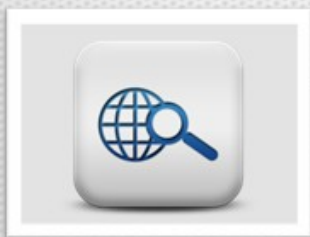
- Sécurisez votre connexion à Internet : WEP au minimum, mais WARP1 ou WARP2 sont plus sûrs. En cas de piratage de votre connexion et de téléchargements illégaux, c'est vous qui serez tenu(e) pour responsable.
- Rendez-vous toujours sur le site officiel du concepteur pour télécharger un logiciel, évitez de passer par un site de téléchargement.
- Prenez le temps de vérifier la validité d'un lien de téléchargement et ne cliquez pas sur n'importe quelle bannière : le bon lien est parfois bien caché au milieu d'autres liens ou bannières qui peuvent être dangereux.
- Respectez les licences et les droits d'auteur, ne téléchargez pas de logiciels piratés.



### À NE PAS FAIRE

- Ne téléchargez ou n'activez jamais un logiciel qui affiche une alerte de sécurité ou une proposition de scan gratuit de votre ordinateur dans le navigateur.
- Évitez de télécharger des applications pour mobiles (sur les réseaux sociaux notamment) dont vous ne pouvez pas vérifier le sérieux.
- Méfiez-vous des lecteurs de vidéos proposés sur les sites de streaming gratuits, ils sont la plupart du temps susceptibles d'injecter un programme malveillant dans votre ordinateur.
- Évitez les sites de téléchargement ou de streaming gratuits, préférez les plateformes de téléchargement légal officielles agréées comme le site [Offre légale](#). Non seulement ces sites enfreignent le droit d'auteur, mais c'est le meilleur endroit pour récupérer des virus ou être confronté à des contenus pornographiques qui s'affichent de manière intempestive.

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## LES ACHATS EN LIGNE



### À FAIRE

- Vérifiez le sérieux du site de vente en ligne : mentions légales obligatoires, coordonnées de contact (téléphone et adresse postale), garanties, service client, etc.
- Prenez contact par téléphone pour vérifier que le numéro de téléphone affiché n'est pas factice et pour prendre quelques garanties.
- Cherchez des avis de clients sur des forums.
- Prévoyez du temps pour effectuer votre achat, ne le faites pas dans l'urgence.
- Au moment de l'achat, vérifiez que l'adresse du site est passée en <https://> et qu'un cadenas est bien présent à côté de l'adresse du site.
- L'achat doit se faire « en deux clics » : 1. la commande et 2. le récapitulatif de la commande, avant de confirmer l'achat.
- Conservez précieusement toutes les données concernant la transaction.

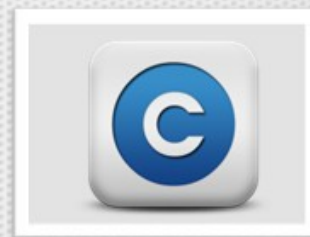
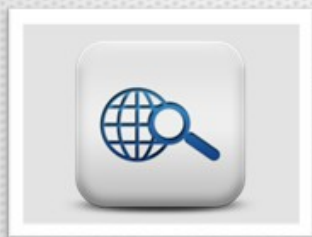


### À NE PAS FAIRE

- Ne communiquez pas vos coordonnées bancaires ailleurs que sur la plateforme sécurisée de paiement (<https://> et cadenas).
- N'effectuez jamais un paiement *via* Western Union ou Mandat Cash, vous n'auriez aucune possibilité de recours en cas de problème.
- Ne cédez jamais à une offre qui semble trop belle pour être vraie, même si les arguments sont convaincants et même si le site semble professionnel.
- Méfiez-vous des sceaux de confiance non officiels, ce ne sont parfois que des images sans garantie associée.
- N'effectuez jamais un achat à partir d'un ordinateur connecté dans un lieu public.



# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## LES RÉSEAUX SOCIAUX



### À FAIRE

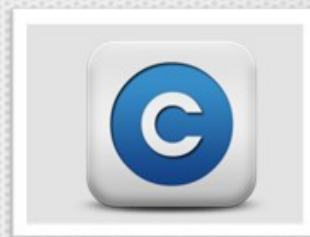
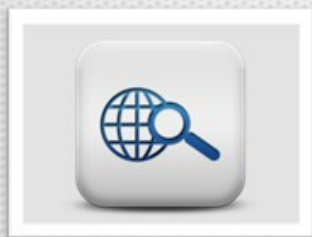
- Sécurisez l'accès à vos comptes de réseaux sociaux avec la validation en deux étapes *via* votre téléphone portable.
- Évitez de remplir tous les champs de votre profil : moins vous en direz et mieux ce sera.
- N'oubliez jamais qu'un réseau social est un lieu public même à l'intérieur d'un groupe « d'amis » et que tout ce que vous diffusez peut être repris et déformé par n'importe qui.
- Autant que possible, n'acceptez comme « amis » que des personnes que vous connaissez dans la « vraie vie » et dont vous avez pu « valider » les comportements.
- Adoptez un ton neutre et ne diffusez que des informations sans implication personnelle.



### À NE PAS FAIRE

- Ne diffusez jamais d'informations trop personnelles sur un réseau social.
- Ne diffusez jamais des photos ou des vidéos personnelles (ou de vos enfants ou proches).
- Ne racontez pas où et quand vous prenez vos vacances, ne donnez aucune indication concernant votre niveau de vie.
- Ne relayez jamais une image ou une vidéo présentant quelqu'un d'autre sans son consentement.
- Ne partagez jamais vos listes de contacts avec un réseau social et n'activez pas la connexion de vos différents réseaux sociaux entre eux.
- Ne vous laissez pas emporter par votre humeur et ne rentrez pas dans une spirale d'invectives lorsque le ton des échanges monte.
- Ne vous repliez pas sur vous-même si vous (ou votre enfant) êtes victime de harcèlement, [parlez-en](#) et, le cas échéant, si les choses s'aggravent, portez plainte.

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## PROTECTION DE LA VIE PRIVÉE



### À FAIRE

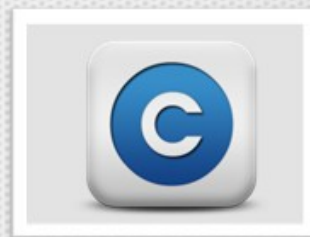
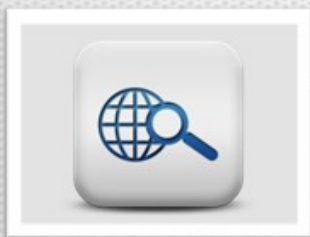
- Déconnectez votre webcam quand vous ne l'utilisez pas (ou tournez-la vers un mur ou masquez-la avec un sparadrap).
- D'une manière générale, pensez à éteindre et à déconnecter vos appareils régulièrement.
- Vous pouvez aussi décider de ne pas emporter votre téléphone portable (smartphone ou tablette) partout où vous allez, sauf bien sûr si vous souhaitez être tracé(e) en permanence !
- Effacez les métadonnées des photos que vous prévoyez de diffuser sur Internet (voir le chapitre « Moteurs de recherche »).
- Utilisez un moteur de recherche anonyme pour vos requêtes ([Startpage](#) pour obtenir les résultats de Google ou [DuckDuckgo](#)).
- Désactivez la fonction de localisation de votre smartphone (tablette ou autre) quand son usage ne s'impose pas.
- Utilisez des pseudos sur les tchats, les forums et les blogs, même si ce n'est pas la panacée absolue, et ne donnez aucune information personnelle (adresse, téléphone, mail, établissement scolaire notamment).



### À NE PAS FAIRE

- Évitez de vous laisser prendre en photo (ou filmer) sans votre consentement. Vous ne pouvez pas savoir quel usage pourra en être fait.
- N'acceptez jamais de vous dénuder devant votre webcam, même si vous pensez qu'une relation intime est en train de se nouer avec quelqu'un que vous avez « rencontré » sur Internet. Vous pourriez vous retrouver piégé(e) par un maître chanteur.
- Ne racontez pas votre vie personnelle sur des blogs, des tchats ou des forums.

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## SAUVEGARDE ET STOCKAGE DES DONNÉES



### À FAIRE

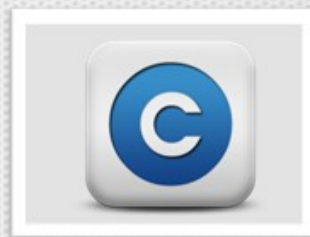
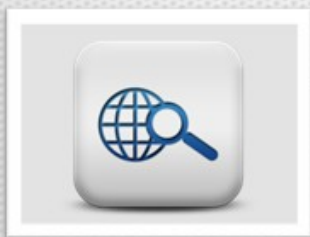
- Sauvegardez vos données personnelles et confidentielles (nom, prénom, date et lieu de naissance, adresse, numéro de sécurité sociale, numéros de compte et de carte bancaire, factures...) ailleurs que dans votre ordinateur. Il suffit de très peu de choses pour usurper votre identité et effectuer des démarches ou des fraudes en votre nom.
- Sauvegardez vos fichiers et données informatiques importants de préférence sur un disque dur externe ou sur un CD/DVD.
- Pour un stockage de vos données en ligne, préférez un service de stockage dont les serveurs se trouvent **sur le territoire français**, comme [hubiC](#) ou [Cloudwatt](#).



### À NE PAS FAIRE

- Ne laissez pas activé le stockage en ligne par défaut de votre smartphone/tablette : en tout état de cause, vos fichiers partent directement sur des serveurs américains et sont donc soumis à la loi [Patriot Act](#). Reprenez le contrôle de vos données et de leur stockage en ligne et ne les laissez pas migrer vers des serveurs américains.

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## COMMUNICATION SUR INTERNET



### À FAIRE

- Faites de votre mieux pour respecter la [Netiquette](#).
- N'oubliez pas qu'Internet est un espace public et que vous ne pouvez jamais savoir par qui vous serez lu. Soignez votre manière de rédiger, soignez l'orthographe !
- Le respect d'autrui doit être une règle absolue, ne vous mettez pas en difficulté en rentrant dans une discussion polémique, vous risquez de ne pas en maîtriser les développements ou les conséquences.
- La courtoisie et la politesse sont de rigueur. Si vous restez courtois(e), vos interlocuteurs le seront aussi.

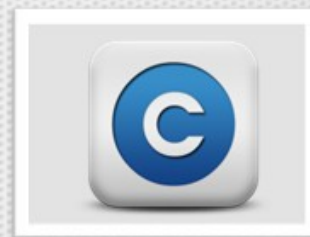
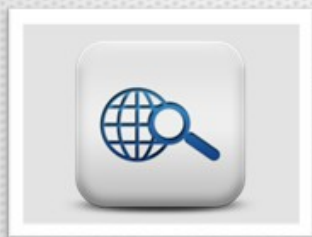


### À NE PAS FAIRE

- N'exprimez rien sans avoir mûrement réfléchi à ce que vous dites et aux possibles conséquences. N'oubliez pas que tout ce qui a été publié sur Internet demeure potentiellement visible éternellement.
- Ne répondez pas aux insultes par des insultes et évitez de prendre parti dans une discussion violente. Analysez froidement la situation, faites la part des choses et ne vous mêlez pas des échanges virulents qui ne vous concernent pas.
- Ne vous liez pas d'amitié avec un(e) inconnu(e) sans l'avoir « validé(e) » dans la « vraie vie » pendant plusieurs mois, voire plusieurs années. Le Web est un terrain de chasse pour les manipulateurs pervers (et les pervers tout court) dont l'habileté principale consiste à séduire en cachant leur jeu. Il est pratiquement impossible de les démasquer avant d'avoir commencé à subir leurs assauts de destruction.



# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## MARKETING (ET) INTERNET



### À FAIRE

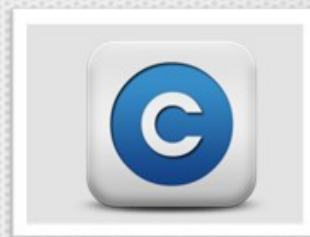
- Efforcez-vous de toujours garder la tête froide : les techniques de vente sur Internet sont particulièrement puissantes et peuvent vous amener à acheter des choses dont vous n'avez pas besoin sans que vous vous en rendiez compte.
- Exercez votre sens critique : une offre trop belle pour être vraie l'est probablement.
- Prenez le temps avant d'acheter quoi que ce soit, même si le marketing mis en œuvre vous met la pression avec une offre à durée limitée. Dites-vous que d'autres offres intéressantes se présenteront tôt ou tard et que, s'il ne s'agit pas d'un achat de première nécessité, mieux vaut attendre d'avoir de vraies bonnes raisons d'acheter.
- La vente sur Internet est soumise en principe aux mêmes exigences que la vente par correspondance. Prenez des garanties avant d'acheter quoi que ce soit.



### À NE PAS FAIRE

- Ne cédez pas aux messages qui prétendent qu'il est facile de gagner de l'argent sur Internet : même si cela est possible, ce n'est ni facile ni rapide, cela demande de très nombreuses compétences et des savoir-faire complexes qui résultent de nombreuses années d'expérience. En outre, nombre de ces annonces sont des arnaques.
- Ne croyez pas tout ce que vous lisez : il n'y a rien de plus facile sur Internet que de se faire passer pour quelqu'un qu'on n'est pas.
- Évitez de vous laisser fasciner par des « beaux parleurs » : le marketing sur Internet fonctionne parce qu'il s'appuie sur le charisme supposé de certains manipulateurs de génie.

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## ASPECTS LÉGAUX



### À FAIRE ou À SAVOIR

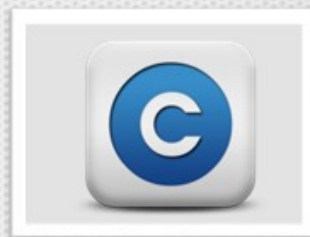
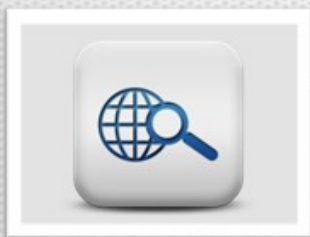
- Respectez la loi exactement comme vous le feriez dans la « vraie vie » : la loi s'applique sur Internet exactement de la même façon que dans le monde physique.
- Respectez les droits d'auteur : demandez toujours l'autorisation à l'auteur d'employer ses contenus (textes, photos, etc.) et citez-le là où vous utilisez ses contenus si aucune mention n'est faite en matière d'utilisation par des tiers.
- Les infractions suivantes sont passibles de 5 ans d'emprisonnement et de 300 000 € d'amende : intrusion dans un ordinateur ou un réseau ; contrefaçon de logiciels ou de bases de données ; téléchargements illégaux ; piratage de réseau téléphonique ; modification ou suppression de données ; défaut de sécurisation des données personnelles ; collectes frauduleuses, illicites ou déloyales de données à caractère personnel.
- Diffuser des images de quelqu'un sans son autorisation peut valoir 1 an d'emprisonnement et 45 000 € d'amende, plus le versement de dommages et intérêts.



### À NE PAS FAIRE

- Ne plagiez pas le travail de quelqu'un d'autre pour vous en servir à votre propre compte.
- Ne téléchargez pas, ne copiez pas, n'utilisez pas et ne diffusez pas un « objet » sans avoir vérifié les termes d'utilisation et les droits d'auteur.
- Ne téléchargez pas et n'utilisez pas un logiciel propriétaire « cracké ».
- Ne portez pas atteinte à la dignité et à l'intégrité d'autrui par des injures, de la diffamation, du harcèlement...

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## CONCLUSION

Après la lecture de ce guide, vous devriez déjà pouvoir modifier plusieurs de vos habitudes de navigation et d'usage d'Internet.

Ce n'est qu'un début. Il existe en effet d'autres nombreuses notions à connaître et à intégrer dans votre conscience de cet environnement numérique, il existe aussi d'autres nombreux outils (gratuits pour la plupart) susceptibles de vous aider à reprendre le contrôle sur votre façon d'être connecté(e).

Il ne s'agit pas de disposer de moyens financiers importants ou d'acquérir des compétences techniques compliquées pour apprendre à se protéger et à naviguer sereinement dans un environnement où nous sommes tracés partout et tout le temps, il s'agit juste de prendre le temps d'intégrer les bonnes notions, de décider d'arrêter d'utiliser certains outils qui mettent en péril la confidentialité de nos données, et de décider d'être actif dans le choix et la configuration des outils informatiques que l'on utilise.

On peut s'indigner du fait que personne ne songe à former les internautes en même temps qu'on leur vend un accès à Internet, il faut juste comprendre qu'il en va de l'intérêt des entreprises du Web de maintenir les internautes dans une certaine ignorance, dans un certain état d'innocence.

Lorsqu'on aborde la question des « dangers d'Internet », le plus souvent on ne pense qu'aux virus, aux escrocs et aux pervers, ce qui ne constitue qu'une toute partie des problèmes à appréhender en réalité.

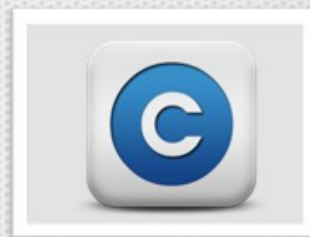
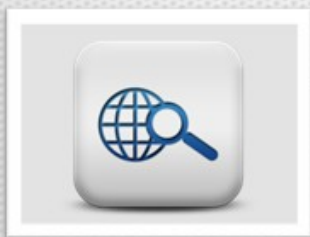
Avoir une approche globale qui couvre toutes les thématiques impliquées dans cet environnement connecté suppose d'avoir passé plusieurs années à évoluer dans ce milieu, à l'avoir observé, à l'avoir vu évoluer.

Ce sont 10 ans d'expérience sur Internet que je mets à votre service dans la [formation](#) que j'ai conçue, pour vous permettre d'avoir une vision plus claire de ce qui se passe dans les coulisses d'Internet.

Parce que savoir, c'est pouvoir. Pouvoir choisir de quelle façon vous interagissez avec Internet, pouvoir vous affranchir des pressions commerciales, pouvoir retrouver la liberté d'aller et venir sans être tracé(e) tout le temps et partout, pouvoir garder le contact avec la « vraie vie », pouvoir avoir de vrais amis et pas seulement des contacts virtuels, pouvoir retrouver du temps pour vous et vos proches...

Ça vaut la peine, non ? :-)

# ÉVOLUER SUR INTERNET EN TOUTE CONFIANCE... ÇA S'APPREND !



## RESSOURCES ET LIENS UTILES

Cette liste n'est qu'un tout petit aperçu de toutes les ressources listées dans la version complète de la formation que j'ai développée (plusieurs dizaines de références d'articles, de sites, de forums, d'outils, etc.), mais vous avez ici plusieurs sites à conserver précieusement dans vos favoris pour vous y référer en cas de besoin.

- Le site de la [CNIL](#) (Commission nationale de l'informatique et des libertés).
- Deux sites pour faire valoir ses droits en matière de commerce transfrontalier : [Econsumer](#) et le [Centre européen de la consommation](#).
- Le site [Soyez net sur le net !](#) : [fiches pratiques](#) sur Facebook et [un test](#) à effectuer.
- [Just Delete Me](#) : un annuaire de liens pour supprimer vos comptes sur différents sites Web.
- Pour les enfants et les jeunes : [NetLa – Mes données m'appartiennent](#).
- Droit des nouvelles technologies : [Legavox](#).
- Évelyne Moreau et Sophie Lorenzo : [Le droit d'auteur et le droit à l'image](#).
- Site officiel [Agir contre le harcèlement à l'école](#).