





## Familles et numérique

Surfer et acheter en toute sécurité



# Sommaire

Page

<b>I - Surfer en toute sécurité</b>	<b>1</b>
1. Définition	2
2. Le paramétrage et la sécurité de l'ordinateur	2
 Zoom sur les cookies, traceurs, vers et spams	4-5
3. Les différents modes de connexion	5
4. La gestion des données personnelles	7
 Zoom sur les risques	8
<b>II - Acheter en toute sécurité</b>	<b>9</b>
1. Les précautions préalables à l'achat en ligne	10
 Zoom sur la sécurité des sites marchands	10
2. Le contrat de vente	12
 Zoom sur l'achat à distance entre particuliers	14
<b>III - Utiliser Internet en famille</b>	<b>15</b>
1. Les nouvelles façons de se connecter	16
2. Les informations et les contenus sur Internet	17
3. Le contrôle parental	19
4. L'utilité d'Internet	20

## Fiches

Mes outils pratiques :

1. Les dix règles d'or de la navigation sur Internet
2. Mes mots de passe, mode d'emploi
3. La sécurité et la maintenance de l'ordinateur
4. La suppression des données et des traces sur Internet
5. Mes lettres types
6. Mes mots-clés
7. Les structures et les sites ressources



## Surfer en toute sécurité



### Les règles d'or de la navigation sur Internet :

- ❑ utiliser un mot de passe complexe pour chaque compte ouvert ;
- ❑ mettre à jour le système d'exploitation et les logiciels ;
- ❑ effectuer des sauvegardes régulières ;
- ❑ utiliser un compte utilisateur plutôt que le compte administrateur pour naviguer sur Internet ;
- ❑ contrôler la diffusion d'informations personnelles en paramétrant l'ordinateur.



## I. Définition



**Surfer** : c'est naviguer sur le web afin de rechercher des informations, de visionner des vidéos, d'écouter de la musique, etc.



## II. Le paramétrage et la sécurité de l'ordinateur

Pour assurer la sécurité des données personnelles, il est important, en premier lieu, d'installer un anti-virus puis de le paramétrer ainsi que l'ordinateur en lui-même, afin de choisir les modalités de leur fonctionnement. Il est primordial également de paramétrer son navigateur Internet.



À savoir :

Quelques règles d'usage :

- définir un compte administrateur et un compte différent pour chaque utilisateur. Le compte administrateur ouvre tous les droits de gestion de l'ordinateur ;
- utiliser un autre compte que le compte administrateur pour naviguer sur Internet. Les risques d'infection ou de compromission sont réduits en limitant les droits d'un utilisateur ;
- dans le navigateur, désactiver par défaut les composants ActiveX et JavaScript et les activer seulement au cas par cas, en fonction des besoins. S'ils permettent d'exécuter certains programmes dans le navigateur, ils peuvent aussi permettre à des programmes malveillants de s'installer facilement ;
- choisir un mot de passe pour chaque compte ouvert. Ce mot de passe doit être complexe<sup>(\*)</sup>.

(\*) Se reporter à l'outil pratique 2 : mes mots de passe, mode d'emploi.

## 1 Les anti-virus et pare-feu

Les logiciels d'anti-virus sont conçus pour identifier, neutraliser et éliminer les logiciels malveillants. Une fois détecté et localisé, l'anti-virus peut supprimer le fichier contaminé ou le mettre en quarantaine pour éviter que le virus ne se répande.

Les anti-virus possèdent des fonctionnalités différentes et doivent être choisis selon sa propre utilisation d'Internet. Il en existe des gratuits et des payants.

Le pare-feu est complémentaire de l'anti-virus car son rôle est de contrôler le réseau et de bloquer les communications intempestives.



**Attention :**

ne jamais utiliser deux anti-virus à la fois car cela empêche leur bon fonctionnement.

## 2 Les mises à jour

Les mises à jour servent à améliorer le rendement et l'efficacité des logiciels de bureautique, des anti-virus, des logiciels de contrôle parental, etc.

Elles améliorent également la sécurité car elles réparent des erreurs constatées sur le logiciel, le rendant ainsi moins vulnérable à des actes malveillants.

Les logiciels disposent d'une fonction de mises à jour automatique qui permet de télécharger et d'installer les correctifs dès qu'ils sont disponibles. Il est conseillé de vérifier malgré tout, la bonne installation de ces mises à jour.



**Attention :**

ne pas confondre les mises à jour avec les mises à niveau. Les mises à niveau sont payantes et non obligatoires. Elles permettent d'obtenir une version plus récente d'un logiciel.



## ZOOM sur les cookies, traceurs, vers et spams

### 1. Cookies et traceurs :

Les cookies sont des traceurs déposés lorsque l'internaute affiche une page Internet, lit un courriel électronique, installe ou utilise un logiciel ou une application mobile.

Ces traceurs permettent aux entreprises d'analyser les habitudes de l'internaute et de lui proposer des publicités ciblées ou des services personnalisés.

Certains cookies sont soumis à obligation de consentement préalable, notamment :

- ☑ ceux liés aux opérations relatives à la publicité ciblée ;
- ☑ les cookies de mesure d'audience ;
- ☑ les cookies traceurs des réseaux sociaux générés par les « boutons de partage de réseaux sociaux ».

L'obligation de consentement consiste à informer les internautes de la finalité des cookies, obtenir leur consentement et à leur fournir un moyen de les refuser.

Le consentement a une durée de validité de 13 mois.

### 2. Spams :

C'est un courriel non sollicité par son destinataire et source d'une gêne manifeste (pourriel). Le spam encombre les boîtes mails, a des contenus parfois inappropriés (image violente). Ils peuvent également être des courriels malveillants et il y a parfois un risque de filoutage ou de phishing<sup>(\*)</sup>.

Les pourriels peuvent prendre la forme de simple publicité.

- ☑ Pour s'en préserver : créer plusieurs adresses de messagerie différentes et les utiliser selon des groupes de relations (famille, amis, clients/fournisseurs...) ;
- ☑ se désabonner des lettres d'information qui ne sont plus intéressantes ;
- ☑ ne jamais répondre à un pourriel ;
- ☑ ne pas programmer de réponses automatiques qui vont répondre aux spams.

<sup>(\*)</sup> Pour plus d'informations : zoom sur les risques.



## ZOOM sur les cookies, traceurs, vers et spams

### 3. Vers :

Un ver est un logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles. Il peut détruire des données, modifier des programmes et utiliser inutilement, parfois intensivement, les ressources de la machine de la victime (réseau, processeur, mémoire, disque).

Afin de se protéger des vers, il convient de mettre à jour systématiquement son système d'exploitation ainsi que les logiciels installés.



## III. Les différents modes de connexion

### 1 Les techniques de connexion

Il existe trois principales techniques de connexion :

- ☒ une connexion par câble Ethernet relié à la box ;
- ☒ une connexion par CPL (Courant porteur en ligne) à partir de deux boîtiers. Le premier est connecté à la box via un câble Ethernet qui envoie un signal par le courant électrique à un second boîtier, lui-même relié par câble Ethernet à l'ordinateur ;
- ☒ le wifi qui permet de se connecter sur Internet depuis n'importe quel ordinateur, tablette, console de jeux ou mobile. C'est donc un outil pratique pour l'ensemble du foyer mais il est primordial de protéger le réseau de l'extérieur(\*) :
  - en changeant le mot de passe utilisateur du routeur Wifi donné initialement. Le mot de passe doit être complexe(\*\*),
  - en changeant le nom du réseau (SSID) afin qu'il soit caché des utilisateurs mal intentionnés. Pour cela, il est conseillé de ne pas utiliser son nom ou son prénom. Désactiver ensuite la diffusion du nom SSID du réseau sans fil en cochant la case correspondante, pour qu'il n'apparaisse pas dans la liste des connexions possibles des personnes étrangères au foyer,

(\*) Se reporter à l'outil pratique 7 : les structures et les sites ressources.

(\*\*) Se reporter à l'outil pratique 2 : mes mots de passe, mode d'emploi.

- en activant le cryptage du réseau (clé de sécurité). Avant d'utiliser le réseau sans fil, il est utile de le crypter avec une clé numérique afin de ne laisser l'accès qu'aux utilisateurs disposant de celle-ci. La manipulation est simple car le cryptage numérique est créé à partir d'une phrase (cinq lettres minimum) et le routeur va générer différents codes qui seront utilisés pour connecter chaque ordinateur du réseau,
- en filtrant les adresses MAC(\*) des ordinateurs, tablettes ou mobiles du foyer pour que seuls ces appareils soient reconnus sur le réseau sans fil,
- en configurant les machines Wifi en fonction des changements effectués (mots de passe, nom du réseau, clé de cryptage).

## 2 Les outils de connexion

Aujourd'hui, il est possible de se connecter via de très nombreux supports tels qu'un ordinateur, un smartphone, une tablette, une console de jeux ou la télévision.

Quelque soit l'outil de connexion, pour une utilisation en toute sécurité :

- ☑ installer un anti-virus quand cela est possible ;
- ☑ vérifier les applications avant de les télécharger en lisant les conditions d'utilisation dans lesquelles sont précisées les données collectées et leur utilisation ;
- ☑ éviter d'enregistrer des informations confidentielles telles que les codes secrets ou les coordonnées bancaires sur le téléphone ou la tablette ;
- ☑ installer un contrôle parental lorsque cela est possible.



### Attention :

définir un code verrouillage permet de protéger les informations du téléphone en cas de perte ou de vol. Le code pin ne suffit pas.

## 3 Les lieux de connexion

Au sein des lieux publics grâce au Wifi libre. Il faut faire attention car la connexion n'est pas protégée. Il est préférable de ne pas lire ses e-mails et de ne pas faire d'achats en ligne à partir d'une connexion dans un lieu public.

Au sein des cybercafés. À la fin de chaque utilisation, effacer l'historique sur le navigateur et fermer la session systématiquement.



### À savoir :

le propriétaire d'un cybercafé, d'un restaurant ou d'un hôtel est tenu de conserver les données trafic de ses clients pendant un an mais il n'est pas obligé d'identifier l'utilisateur. Les données trafic concernent l'adresse IP de l'ordinateur, la date, l'heure, et la durée de chaque connexion.

(\*) Se reporter à l'outil pratique 6 : mes mots clés.





## IV. La gestion des données personnelles

Les données personnelles sont toutes les informations qui permettent d'identifier une personne telles que son identité, son adresse, une photo mais aussi des données qui concernent sa santé, ses opinions religieuses et politiques, ses origines, etc.

À chaque navigation sur Internet, un certain nombre d'informations sont enregistrées telles que l'adresse IP, l'historique de navigation, les mots clés saisis sur un moteur de recherche. Ces informations collectées pourront notamment servir entre autres à des régies publicitaires ou des éditeurs de services pour proposer à l'internaute des publicités et des services personnalisés.

Il est donc important d'être vigilant aux informations demandées par les éditeurs de sites Internet et de lire attentivement la charte de confidentialité.



À savoir :

chaque internaute a le droit d'être informé et d'accéder aux données personnelles le concernant. Il a le droit également de s'opposer ou de demander la rectification de ses données.

### 1 Les réseaux sociaux

L'utilisation des réseaux sociaux comporte des risques, notamment celui de perdre la maîtrise de son identité numérique, puisqu'un nombre très important d'informations personnelles y sont diffusées. Ces données personnelles sont accessibles sans limitation de durée sur Internet. L'internaute a ensuite très peu de maîtrise dessus puisque, une fois publiées, elles peuvent circuler et être exploitées très rapidement, en dehors du réseau d'amis auquel elles étaient initialement destinées.

Pour se prémunir de tout désagrément, il est conseillé de :

- ☑ sécuriser son compte sur les réseaux sociaux en apprenant à maîtriser les paramètres de sécurité de son profil utilisateur ;
- ☑ vérifier régulièrement les paramètres de sécurité du profil car les conditions de confidentialité peuvent changer ;
- ☑ éviter de mettre en ligne des données personnelles ;
- ☑ bien réfléchir avant la publication de photo ou la mise en ligne de commentaires.

Si une atteinte à la vie privée est constatée, elle doit être signalée auprès du réseau social concerné. Il est important de conserver des preuves de ce signalement en effectuant des copies écran. En cas de réponse incomplète, insatisfaisante, voire d'absence de réponse de la part du réseau social, une plainte peut être adressée à la CNIL(\*) contre le réseau social.

(\*) Se reporter à l'outil pratique 7 : les structures et les sites ressources.

## 2 Le cloud-computing

Le cloud computing ou cloud («nuage» en français) désigne un ensemble de processus qui consiste à utiliser la puissance de stockage de serveurs informatiques distants via Internet. Ce service permet à l'internaute de stocker les données qu'il souhaite sur un serveur dédié. Le cloud-computing permet ainsi de rendre les données accessibles partout à condition d'être connecté à Internet et de les partager avec d'autres personnes.

Le prestataire doit apporter des informations claires concernant la sécurité des données hébergées dans le cloud (pays hébergeant les serveurs du prestataire, les garanties de sécurité mises en place). Le prestataire doit également garantir le respect de conservation des données, la destruction ou la restitution de ces données et la coopération avec les autorités de protection des données.



### ZOOM sur les risques

#### 1. Le piratage :

Le piratage correspond au cassage de protection de sécurité de logiciels tels que les boîtes de messagerie, des comptes sur les réseaux sociaux ou bien des fichiers de données personnelles.

#### 2. Le phishing ou filoutage :

Par l'intermédiaire d'un courriel et d'un faux site Internet, le fraudeur essaie d'obtenir les coordonnées bancaires en prenant l'apparence d'une banque ou d'un service connu.



#### Attention :

les demandes d'informations confidentielles ne sont font JAMAIS par courriel. Il ne faut donc pas y répondre et les supprimer.

#### 3. Le vol d'identité :

L'usurpation d'identité consiste à utiliser des données personnelles d'un individu, à son insu pour accéder à l'un de ses comptes et agir en son nom. Il peut s'agir aussi de créer un compte ou un site en utilisant une identité frauduleuse.

Dans ce cas, il ne faut pas attendre pour réagir :

- ☑ en déposant une plainte pénale auprès du commissariat ;
- ☑ en s'adressant au responsable du site afin de demander à consulter les données personnelles détournées ou exiger leur suppression. Si aucune réponse n'est donnée, il est possible d'adresser une plainte en ligne à la CNIL (\*).

#### 4. Le « typosquattage » :

Un site, le plus souvent marchand, utilise un nom très proche d'un site connu afin de créer la confusion chez les consommateurs qui passeront alors des commandes. Ces sites « copieurs » empruntent presque à l'identique l'interface et le nom du site original.

(\* ) Se reporter à l'outil pratique 5 : mes lettres types.



## Acheter en toute sécurité



### Les règles d'or de l'achat en ligne :

- ❑ vérifier l'exactitude de l'adresse du site ;
- ❑ vérifier le niveau de cryptage de la page ;
- ❑ transmettre uniquement les données nécessaires à la transaction ;
- ❑ favoriser les sites Internet connus.



#### Attention :

les recommandations suivantes ne sont valables que pour les sites marchands français, les sites étrangers ne répondant pas à la législation française. Il est donc essentiel de vérifier, avant tout achat, dans la rubrique des mentions légales, l'adresse du siège social et le numéro de téléphone, même pour une marque française.



# I. Les précautions préalables à l'achat en ligne



## ZOOM sur la sécurité des sites marchands

Trois pictogrammes différents apparaissent dans la barre des tâches en fonction du niveau de cryptage de la page :

Cadenas ouvert : lorsque la page n'est pas sécurisée.

Cadenas fermé : lorsque la page est entièrement sécurisée.



Point d'exclamation ou bouclier : lorsque seules certaines zones de la page sont sécurisées.



Votre navigateur a bloqué du contenu non sécurisé.

La plupart des sites web continueront de fonctionner correctement même si ce contenu est bloqué.

Il est important de vérifier :



VENDEUR	1 ARTICLE	DISPONIBILITÉ	QUANTITÉ	PRIX TOTAL
	Passport de la Maternelle Moyenne Section à la Grande Section Collectif	En Stock	- 1 + Supprimer	5,40€
Frais de livraison estimés : .....				0,01 €
choisissez le retrait en magasin à l'étape suivante (choix du mode de livraison) pour bénéficier automatiquement de <b>5% de remise immédiate sur tous vos livres</b> (?)				
✦ Faites-vous livrer en <b>1 jour ouvré*</b> gratuitement. Essai gratuit pendant <b>30 jours sans engagement</b> . <a href="#">En savoir plus</a> <small>*voir conditions</small>			<b>ESSAYER GRATUITEMENT</b>	
	<input type="checkbox"/> EMBALLAGE CADEAU ? Écrire une dédicace			
	<b>Code avantage ou bon de réduction</b> (uniquement sur Fnac.com et Fnacpro.com) : Saisissez le ici... <b>RECALCULER</b> <small>Si vous disposez d'un chèque cadeau, utilisez-le lors du paiement à l'étape 4</small>			

Contactez-nous | Aide | CGV Azerty.com | Protection des données

↑  
mentions légales : adresse du siège du vendeur, numéro de téléphone du vendeur, charte de confidentialité des données

- ❑ les mentions « https » et le cadenas fermé dans la barre des tâches ;
- ❑ les garanties proposées par le site ;
- ❑ l'existence d'une adresse postale (hors boîte postale).

Le certificat d'authentification du site ne s'affiche que s'il y a un problème. Dans ce cas, il ne faut pas effectuer la transaction. Pour vérifier l'existence réelle du vendeur, en complément de la vérification des mentions légales, il est possible de lire les avis des internautes.

Avant de valider la commande, vérifier que le cryptage de la page d'envoi des coordonnées bancaires soit bien effectif.

Éviter d'enregistrer les coordonnées bancaires sur un site Internet (compte de paiement) d'un commerçant même pour faciliter les achats ultérieurs. Lors d'un premier achat, si l'enregistrement des coordonnées bancaires est obligatoire, il est possible d'effacer les données en vous connectant à votre compte de paiement.



**Conseil :**

taper l'adresse du site marchand souhaité dans la barre de recherche et partir de la page d'accueil du site pour naviguer sur les autres pages. Ne jamais cliquer sur un lien reçu dans un mail.



## II. Le contrat de vente

La commande doit être présentée en trois étapes :

1. visualisation du détail de la commande (le prix doit être TTC et doit être exprimé en euros) ;
2. correction d'éventuelles erreurs ;
3. confirmation de la commande en général par courriel avec le récapitulatif détaillé de la commande.



### Attention :

en cas de non-conformité du produit, il est conseillé d'envoyer au vendeur un courrier en lettre recommandée afin d'obtenir le remboursement ou l'échange du produit. Il est possible également de contacter une association de consommateurs<sup>(\*)</sup>.

### 1 Les droits et obligations du vendeur

Le vendeur est entièrement responsable de la bonne exécution du contrat conclu à distance y compris de la livraison. Il doit indiquer la date limite à laquelle il s'engage à livrer le bien ou à exécuter la prestation de service. Il doit informer le client de tout retard.

Si la livraison est non conforme ou défectueuse, le vendeur doit reprendre les articles en question. Les frais sont à la charge du vendeur. Plusieurs possibilités s'offrent à lui telles que procéder à une nouvelle livraison en respectant la commande, réparer le bien défectueux, échanger le produit, ou rembourser la commande en cas d'annulation.



### Conseil :

vérifier l'état de l'emballage et du produit au moment de la livraison. Si cela n'a pas été fait, l'acheteur dispose de trois jours pour émettre des remarques au transporteur par lettre recommandée.

<sup>(\*)</sup>Se reporter à l'outil pratique 7 : les structures et les sites ressources.

## 2 Les droits de l'acheteur

Pour faire valoir ses droits, l'acheteur doit se reporter au contrat de vente dans lequel sont définis les recours possibles qui peuvent différer selon le vendeur et la nature du produit acheté. Il convient donc de le lire minutieusement avant de procéder à l'achat.

## 3 Les moyens de paiement en ligne

Tous les paiements par Internet doivent s'effectuer dans une zone cryptée, c'est-à-dire que l'adresse URL doit commencer par « https ».

Paiement par carte bancaire : seuls le numéro de carte bancaire, la date d'expiration et le cryptogramme visuel sont nécessaires à la transaction.

En cas d'utilisation frauduleuse, le titulaire de la carte doit agir au plus vite auprès de sa banque pour faire opposition au paiement.



### Attention :

ne jamais donner, lors d'un achat en ligne, le code confidentiel de la carte bancaire qui ne sert que pour les paiements dans les magasins et les retraits au distributeur.

Porte-monnaie électronique : il existe deux types de porte-monnaie électronique :

- ☒ un porte-monnaie qui stocke de la monnaie sans passer par un compte bancaire, de la même façon que le système monéo. Le système existe par carte à puce, par le téléphone mobile mais aussi par clé USB. Cela permet à l'utilisateur de faire des achats sur Internet en toute sécurité ;
- ☒ un porte-monnaie sécurisé permettant d'initier un virement de son compte vers celui d'un fournisseur, via un terminal de paiement. Dans ce cas, il s'agit d'un substitut à la carte bancaire traditionnelle et le porte-monnaie électronique permet alors d'accéder simplement à son compte bancaire de façon sûre (Google Wallet, paypal).



## ZOOM sur l'achat à distance entre particuliers

Les achats et les ventes entre particuliers sont le plus souvent conclus via des plateformes de ventes. Les ventes sont réalisées à prix fixe ou sous forme d'enchères.

Lors d'un achat avec un particulier, l'acheteur n'a aucune garantie. Il est donc important d'être vigilant et d'éviter le paiement en liquide, par transfert de fonds ainsi que l'envoi de pièces ou de billets par voie postale.



### Conseil :

sur de nombreuses plateformes de vente, il est possible de se renseigner sur la réputation du vendeur, en lisant les avis d'internautes qui ont déjà conclu une vente avec ce dernier.

Il est préférable de passer par les sites ayant des partenariats avec des sociétés d'assurance et/ou ayant mis en place un système de garantie avec des franchises et un plafond.



### Attention :

pour la location entre particuliers, il est essentiel d'attendre le contrat de location avant de verser un acompte.





## Utiliser Internet en famille



### Les règles d'or de l'apprentissage d'Internet :

- ❑ orienter les enfants vers les sites Internet appropriés à leur âge ;
- ❑ vérifier systématiquement la source des informations ;
- ❑ faire attention à ce qui est écrit ou publié sur les blogs et les réseaux sociaux ;
- ❑ vérifier les autorisations avant d'utiliser une photo, une vidéo, ou des écrits ;
- ❑ demander systématiquement l'accord de la personne avant de publier une photo la concernant ;
- ❑ ne pas divulguer des informations personnelles ;
- ❑ limiter le temps d'accès à Internet.



# I. Les nouvelles façons de se connecter

Aujourd'hui, il est possible de se connecter sur Internet à partir d'autres appareils que l'ordinateur fixe comme l'ordinateur portable, le smartphone, la console de jeu, la tablette, etc.

Ces appareils ont l'avantage et l'inconvénient d'être mobiles ce qui rend plus difficile le contrôle des parents sur la pratique d'Internet de leurs enfants. Il est donc important d'apprendre aux enfants à s'en servir à bon escient.

Sur Internet, chacun a des droits mais surtout des devoirs. Le premier d'entre eux est de respecter la loi.

## Il est interdit :

- ❑ de pirater des œuvres numériques c'est-à-dire de télécharger illégalement des musiques ou des films ou de contrefaire des logiciels ;
- ❑ de diffamer un professeur, un camarade ou toute autre personne ;
- ❑ de filmer et de mettre en ligne une vidéo d'une agression, de se moquer d'autrui sur les réseaux sociaux ou sur un blog et de porter atteinte à la vie privée d'un tiers (Happy slapping, cyber-harcèlement<sup>(\*)</sup>), sous peine de sanction pénale.

## Il est obligatoire :

- ❑ de demander l'accord de la personne concernée avant toute publication de vidéo ou de photo. Si la personne est mineure, l'autorisation écrite d'un parent ou d'un tuteur est nécessaire.

## Les principaux droits de l'internaute sont :

- ❑ de refuser l'utilisation de ses données personnelles pour l'envoi de publicité ;
- ❑ de refuser la publication d'une photo de soi ou le cas échéant, de les faire retirer ;
- ❑ de réfléchir systématiquement avant l'envoi de photo ou de données personnelles sur les réseaux sociaux par exemple ;
- ❑ de porter plainte en cas d'atteinte à la vie privée, de cyber-harcèlement, ou d'usurpation d'identité.

(\*) Se reporter à l'outil pratique 6 : mes mots clés.



## II. Les informations et les contenus sur Internet

### ① Apprendre à faire le tri dans les informations

Sur Internet, des informations erronées peuvent circuler. Quelques conseils permettent de trier les informations pertinentes :

- ☒ vérifier qui est l'auteur de l'information ;
- ☒ croiser les sources en visitant plusieurs sites Internet, cela permet de se faire son propre avis ;
- ☒ être critique vis-à-vis des contenus ; l'auteur peut influencer le point de vue du lecteur ;
- ☒ éviter les sites personnels ;
- ☒ vérifier la date de publication de l'information.

### ② Les contenus libres de droit : comment les identifier ?



#### Attention :

contenu libre de droits ne veut pas forcément dire gratuit. Il faut parfois payer un droit d'utilisation. Il faut donc bien vérifier les conditions d'utilisation pour éviter tout risque d'infraction au droit d'auteur. Dans tous les cas et pour tous les contenus, l'accord de l'auteur est nécessaire.

Les photos, les textes, les musiques, les vidéos et autres utilisés dans un devoir par exemple doivent être libres de droits c'est-à-dire que chacun, après l'accord de l'auteur et selon les droits qu'il a accordés, peut utiliser librement l'œuvre choisie.

Ainsi il existe plusieurs types de contenus libres de droits :

- ☒ les contenus sous licences « Creative Commons ». Il existe six licences différentes qui permettent à l'auteur d'une image de choisir les droits afférents à l'image accordés aux utilisateurs ;
  - attribution : les utilisateurs doivent mentionner le nom de l'auteur pour toute utilisation de l'œuvre,
  - attribution sans modification,
  - attribution sans modification ni d'utilisation commerciale,
  - attribution et interdiction d'utilisation commerciale,

- attribution, partage dans les mêmes conditions (autorisation à reproduire, diffuser et modifier l'œuvre, à condition que les utilisateurs publient toute adaptation de l'œuvre sous les mêmes conditions que son auteur originel) et interdiction d'utilisation commerciale,
- attribution et partage dans les mêmes conditions.

☑ les contenus et plus particulièrement les images tombées dans le domaine public.

On peut les trouver à partir :

- des sites recensant les images et les autres contenus sous licence « créative-commons » ([http://creativecommons.fr/.](http://creativecommons.fr/)) ;
- de Google grâce à la recherche avancée (seulement pour les images).

Pour cela :

- saisir le mot-clé des images recherchées dans la rubrique image,
- sur la page des résultats, vous allez cliquer sur le bouton sous forme d'écrou (en haut à droite) et sélectionner l'option « Recherche avancée »,
- sur la liste des critères, choisir « droits d'usage » et sélectionner le type de fichier souhaité. Il est recommandé de choisir l'option « libre de droits d'usage ou de distribution ».

### 3 Les logiciels libres(\*)

Les logiciels libres sont des programmes informatiques libres de droits c'est-à-dire que chacun peut les utiliser, les améliorer et les diffuser comme il le souhaite. C'est une offre alternative à l'offre payante classique.

Il en existe de tous types comme par exemple, pour la bureautique (traitement de texte notamment) mais également pour gérer son budget (logiciel de comptabilité).

Il est possible également de télécharger des logiciels sur une clé USB. Cela permet, sans se connecter à Internet, de les utiliser en toute sécurité. Des packs prêts à télécharger peuvent être proposés sur certains sites de logiciels libres(\*).



**Attention :**

le logiciel libre n'est pas forcément gratuit.

(\*) Se reporter à l'outil pratique 6 : mes mots clés.



## III. Le contrôle parental



### À savoir :

les parents sont responsables au niveau civil ou pénal des actes commis sur Internet par leurs enfants mineurs.

### 1 Les logiciels

De nombreux logiciels de contrôle parental existent. Certains sont fournis gratuitement par le prestataire d'Internet, d'autres sont payants. Il est important de vérifier toutes les modalités du logiciel et de les comparer en fonction de ses besoins. En règle générale, ils permettent de fixer des limites horaires en fonction du logiciel utilisé, de l'utilisation de la connexion Internet, ou de l'ordinateur lui-même (arrêt de l'ordinateur). Ils peuvent aussi être paramétrés afin d'interdire l'accès à des sites sensibles (liste noire : pornographie, sites choquants, violents) ou de définir une liste de sites autorisés (liste blanche) mais cette dernière option est très restrictive. Il est possible également de limiter l'accès à des jeux ou à d'autres logiciels de téléchargement ou de messagerie instantanée.



### Attention :

le contrôle parental ne fonctionne pas toujours sur les téléphones portables connectés en wifi.

### 2 Les bons réflexes à transmettre aux enfants

Parce que le contrôle parental ne suffit pas et qu'à terme les enfants et les jeunes doivent être autonomes dans leur utilisation d'Internet, il est important de leur transmettre de bonnes pratiques :

- ☑ leur apprendre leurs droits et leurs devoirs ;
- ☑ discuter de leurs pratiques sur Internet ;
- ☑ les inciter à dialoguer avec un adulte dès qu'ils rencontrent une difficulté.
- ☑ les responsabiliser sur ce qu'ils mettent en ligne ;
- ☑ rappeler les liens entre le monde virtuel et la réalité, les actes commis sur Internet ayant un véritable impact et des conséquences non négligeables dans la vie réelle ;
- ☑ paramétrer ensemble les critères de confidentialité sur les réseaux sociaux notamment ;
- ☑ les sensibiliser sur les risques d'Internet (programmes malveillants, pratiques excessives) ;
- ☑ montrer l'exemple.

### ① Les services en ligne

Les services en ligne regroupent tous types de services (banques, services publics, administrations). Ils facilitent l'accès aux usagers qui n'ont, de fait, plus besoin de se déplacer pour obtenir des informations ou entreprendre certaines démarches. Ces services en ligne permettent aux institutions, aux entreprises et aux usagers de gagner du temps dans leurs démarches. L'internaute peut ainsi trouver des formulaires ou des services en ligne tels que la possibilité de déclarer ses impôts.

**Attention :**

se méfier des sites qui copient l'interface web d'une institution ou d'une banque. Pour cela, il est nécessaire de toujours de vérifier l'adresse URL du site consulté.

### ② Les sites Internet pour les enfants et les jeunes

Internet est une source intarissable d'informations. Certains sites permettent de découvrir et d'apprendre de nouvelles choses, il serait dommage d'en priver les enfants et les jeunes. Il faut donc les orienter, les aider à découvrir et à adopter des sites et contenus en ligne de qualité appropriés à leur âge.

Sur le site, [www.panelparents.fr](http://www.panelparents.fr), une sélection de sites Internet, classés en fonctions des âges des enfants, des thématiques et de la langue, est proposée aux parents. Ainsi, il est possible de retrouver aussi bien des jeux que des sites pédagogiques ou d'informations, qui leur permettent de communiquer entre eux ou de se divertir.

Toute mise à jour de contenu sera disponible, le cas échéant, sur : [www.udaf91.fr](http://www.udaf91.fr)

L'Udaf de l'Essonne agit pour la défense des intérêts matériels et moraux des familles. Elle est à la tête d'un réseau de plus de 60 associations familiales et fonde son avis et son action sur leur expérience.

La collection de guides pratiques a donc été conçue pour les familles avec l'objectif de leur apporter un éclairage sur des sujets qui les touchent directement et de leur permettre d'agir avec prudence et discernement.

« Familles et numérique : surfer et acheter en toute sécurité » est le second guide de la collection. Y sont abordés à la fois les différentes utilisations d'Internet ainsi que de multiples conseils pratique pour une navigation optimale en famille.

Les guides pratiques de l'Udaf de l'Essonne :

N°1 Emprunts – crédits : comment s'y retrouver ?

N°2 Familles et numérique : surfer et acheter en toute sécurité



Udaf de l'Essonne  
315, square des Champs-Élysées BP 107  
Courcouronnes  
91004 Évry  
Tel. 01 60 91 30 30  
<http://www.udaf91.fr>

1. Utiliser un mot de passe complexe pour chaque compte ouvert ;
2. utiliser systématiquement le compte utilisateur pour naviguer sur Internet ;
3. trier les informations pertinentes en croisant les sources de différents sites Internet, en choisissant des auteurs sérieux et en vérifiant les dates de publication ;
4. protéger ses données personnelles et ne transmettre que ce qui est nécessaire lors d'achat en ligne ou lors d'une inscription à des sites Internet ;
5. sur les réseaux sociaux, bien choisir son pseudo et bien paramétrer son profil et son compte de confidentialité ;
6. réfléchir avant toute publication de commentaires, photos ou vidéos ;
7. respecter systématiquement le droit à l'image et le droit d'expression ;
8. dès qu'un contenu choquant apparaît, éteindre immédiatement l'écran, en discuter avec un adulte et signaler les pages correspondantes ([www.pointdecontact.net](http://www.pointdecontact.net)) ;
9. éviter d'accepter des rendez-vous avec des inconnus ou le cas échéant, y aller accompagné et choisir un lieu de rencontre public et fréquenté ;
10. en cas de harcèlement sur Internet, prévenir immédiatement un adulte, faire retirer les commentaires ou photos des sites Internet et porter plainte.





## Mode d'emploi

1. Utiliser des caractères variés et spéciaux : majuscules, minuscules, chiffres, symboles (+, », &) et marques de ponctuation ;
2. composer le mot de passe avec au minimum huit caractères ;
3. créer un mot de passe complexe en évitant d'utiliser ses données personnelles telles que sa date de naissance ou son nom ;
4. créer un mot de passe facile à mémoriser en choisissant une phrase ;
5. Différencier les mots de passe de chaque compte en ajoutant la première et la dernière lettre du nom de domaine.



## Exemple

1. Choisir une phrase :

Choisir **un mot de passe complexe et sécurisé**.

2. Prendre les premiers caractères des mots et utiliser différents caractères :

Mot de passe créé : C1mdpc&s.

3. Ajouter la première et la dernière lettre du nom de domaine :

Par exemple : [www.udaf91.fr](http://www.udaf91.fr)

Mot de passe créé : C1mdpc&s.u1



## Conseil :

- ❑ ne pas stocker les mots de passe sur l'ordinateur, les écrire sur un papier ou se les envoyer par courriel ;
- ❑ supprimer systématiquement les courriels envoyés lors d'une création de compte sur Internet ;
- ❑ configurer, au cas par cas, les logiciels pour qu'ils ne se « souviennent pas » automatiquement des mots de passe.

**Conseil :****Pour la maintenance de l'ordinateur :**

- ☒ installer un logiciel antivirus ;
- ☒ effectuer régulièrement les mises à jour du système d'exploitation et de l'antivirus ;
- ☒ effectuer des sauvegardes régulières des données sur des supports externes (clés USB, disques durs externes, DVD gravés, etc.) ;
- ☒ désinstaller les logiciels non utilisés ;
- ☒ supprimer les fichiers inutiles et vider la corbeille.

**Conseil :****Pour garantir la sécurité de l'ordinateur :**

- ☒ surfer sur Internet à partir du compte utilisateur uniquement ;
- ☒ vérifier systématiquement l'expéditeur d'un courriel ;
- ☒ ne pas ouvrir les pièces jointes d'un courriel envoyé par un expéditeur inconnu ;
- ☒ vérifier l'adresse d'un lien Internet en passant la souris dessus ;
- ☒ ne télécharger que des programmes connus ou, à défaut, des programmes distribués par des sites connus ;
- ☒ stopper aussitôt l'activité en cours lorsqu'une alerte se déclenche dans le navigateur ou bien directement dans une page web ;
- ☒ privilégier les programmes et logiciels libres de droits.

**Se méfier des programmes malveillants :**

Chaque programme a sa technique d'intrusion et d'exploitation de l'ordinateur. Les plus connus sont :

- ☒ **adware** : programme qui affiche des publicités afin de rediriger l'utilisateur vers certains sites web ;
- ☒ **cheval de Troie** : programme tel qu'un économiseur d'écran ou un « faux » antivirus qui sert à cacher un programme malveillant ;
- ☒ **keylogger** : programme qui enregistre les frappes au clavier pour récupérer les mots de passe, les numéros de cartes de crédit ;
- ☒ **spyware** : programme qui collecte des informations sur les internautes à leur insu afin de mieux cibler les publicités.

À chaque navigation sur Internet, un certain nombre d'informations sont enregistrées (cookies) telles que l'adresse IP, l'historique de navigation, les mots clés saisis sur un moteur de recherche.

Les cookies permettent d'identifier les habitudes et les centres d'intérêt de l'internaute ainsi que de le localiser pour notamment proposer des services et faire apparaître des publicités ciblées.

**Conseil :**

en amont de la navigation sur Internet, penser à paramétrer le navigateur afin de bloquer systématiquement les cookies.

Comment effacer ses traces ?

- ☒ se déconnecter de tous les sites visités ;
- ☒ configurer les logiciels pour qu'ils ne se « souviennent pas » des mots de passe automatiquement ;
- ☒ effacer l'historique de navigation ;
- ☒ fermer la session utilisateur notamment lors de connexion dans un cyber-café.

1

Demande de suppression de données personnelles mises en ligne sur un site Internet



Attention :

joindre votre pièce d'identité au courrier.

Madame, Monsieur,

Des informations me concernant sont actuellement diffusées sur votre site Internet à l'adresse suivante : **[Précisez l'Adresse (URL) et la page concernée]**.

La publication de ces informations sur internet porte atteinte à **[Précisez de façon détaillée les motifs pour lesquels vous ne souhaitez pas que ces données soient publiées sur internet]**.

Aussi, conformément à l'article 38 de la loi « informatique et libertés » du 6 janvier 1978 modifiée, je vous remercie de supprimer les informations suivantes **[Décrivez les données personnelles que vous souhaitez faire supprimer]**.

Je vous demande également de faire le nécessaire pour que ces pages ne soient plus référencées par les moteurs de recherche.

Je vous rappelle que vous disposez d'un délai maximal de deux mois suivant la réception de ce courrier pour répondre à ma demande (article 94 du décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée).

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

(Signature)

<sup>(\*)</sup> Source : www.cnil.fr

2

Demande de droit d'accès aux informations contenues dans un fichier

**Attention :**

à envoyer en recommandé avec accusé de réception. Joindre votre pièce d'identité au courrier.

Madame, Monsieur,

Conformément à l'article 39 de la loi du 6 janvier 1978 modifiée en août 2004, je vous prie de bien vouloir m'indiquer si des informations me concernant figurent dans vos fichiers informatisés ou manuels.

Dans l'affirmative, je vous demande de me faire parvenir une copie, en langage clair, de l'ensemble de ces données (y compris celles figurant dans les zones « blocs-notes » ou « commentaires »).

Vous voudrez bien également me donner toute information disponible sur l'origine de ces données me concernant.

Je vous rappelle que vous disposez d'un délai maximal de deux mois suivant la réception de ce courrier pour répondre à ma demande, conformément à l'article 94 du décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

(Signature)

3

Demande de rectification de données figurant dans un fichier

**Attention :**

à envoyer en recommandé avec accusé de réception. Joindre votre pièce d'identité au courrier.

Madame, Monsieur,

Conformément aux dispositions de l'article 40 de la loi du 6 janvier 1978 modifiée en août 2004, je vous prie de bien vouloir rectifier..... ou compléter..... ou mettre à jour..... ou effacer..... (à choisir selon votre situation)

Vous voudrez bien m'adresser copie de l'enregistrement ainsi modifié (alinéa 2 de l'article 40). Pour faciliter le traitement de ma demande, je vous précise que [à compléter]...

Je vous rappelle que vous disposez d'un délai maximal de deux mois suivant la réception de ce courrier pour répondre à ma demande, conformément à l'article 94 du décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

(Signature)

4

Demande de l'intervention de la CNIL lors d'un problème pour exercer son droit d'accès



**Attention :**

joindre les photocopies des courriers adressés à l'organisme détenteur de données avec, éventuellement, photocopies des réponses de cet organisme estimées non satisfaisantes (notamment incomplètes).

Monsieur le Président,

Je souhaite appeler votre attention sur les faits suivants. J'ai exercé mon droit d'accès auprès de [à compléter] par courrier(s) du...(cf. copie(s) ci-jointe(s)).

[à compléter par exemple en indiquant à la CNIL à quelles dates vous avez effectué vos demandes et quelles sont les réponses qui vous ont été faites]

C'est pourquoi je demande à la CNIL de [à préciser]

Je vous prie d'agréer, Monsieur le Président, l'expression de mes salutations distinguées.

(Signature)

(\*) Source : [www.cnil.fr](http://www.cnil.fr)



5

Demande de suppression des coordonnées pour l'arrêt d'envoi de publicités



**Attention :**

ces courriers sont à adresser aux organismes expéditeurs des publicités et non à la CNIL.



**Conseil :**

joindre la dernière publicité.

Madame, Monsieur,

Conformément aux dispositions de l'article 38 alinéa 2 de la loi du 6 janvier 1978 modifiée, je vous demande de supprimer mes coordonnées de vos fichiers d'envoi de publicités.

Je vous rappelle que vous disposez d'un délai maximal de deux mois suivant la réception de ce courrier pour répondre à ma demande, conformément à l'article 94 du décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

(Signature)

<sup>(\*)</sup> Source : [www.cnil.fr](http://www.cnil.fr)

**Adresse IP** : c'est le numéro d'identification qui est attribué à chaque appareil connecté au réseau.

**Adresse mac** : c'est l'adresse de la carte réseau.

**Adresse URL** : elle correspond à l'adresse Web d'un site Internet.

**Certificat SSL** : il assure une connexion sécurisée entre le serveur Web et le navigateur notamment pour les transactions bancaires.

**Compte administrateur** : il ouvre tous les droits de gestion de l'ordinateur (configuration de l'ordinateur et installation de tous les programmes souhaités).

**Compte utilisateur** : il possède moins de droit que le compte administrateur. Il est conseillé d'utiliser ce compte pour surfer et acheter sur Internet.

**Cyber-harcèlement** : ce sont des moqueries répétées d'une autre personne sur Internet notamment sur les réseaux sociaux, et les blogs.

**Données personnelles** : il s'agit de toute information relative à une personne physique qui permet directement ou indirectement de l'identifier (noms, prénoms, adresses, numéro de téléphone, lieu et date de naissance, numéro de sécurité sociale, etc.). Cela regroupe également les données à caractère personnel telles que les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, etc.

**Happy-slapping** : il s'agit d'une vidéo mise en ligne d'une agression.

**Hoax** : ce sont des canulars diffusés sur le web, souvent ce sont de fausses informations envoyées par mail, via les réseaux sociaux ou sur des sites parodiques.

**Logiciel libre** : c'est un programme informatique modifiable par tous qui accordent certains droits aux utilisateurs. Il peut être payant mais son utilisation est libre et chacun peut l'étudier, le modifier ou distribuer des copies.

**Numéro IMEI (International Mobile Equipment Identity)** : c'est un numéro unique qui sert à identifier chaque téléphone.

**Pare-feu** : le pare-feu est complémentaire de l'anti-virus car son rôle est de contrôler le réseau et de bloquer les communications intempestives.

**PDA** : Personal digital assistant. C'est un petit ordinateur de poche.

**Plug-in active X et Java script** : ce sont des programmes qui facilitent la navigation en autorisant une animation ou en aidant dans différentes tâches telles que l'installation de mises à jour de sécurité.

**Puce NFC (near field communication)** : c'est une technologie qui permet à deux appareils électroniques de communiquer entre eux et sans fil lorsqu'ils sont physiquement proches (exemple : paiement sans contact via le téléphone portable).

**SSID** : Service Set Identifier. C'est le nom du Réseau sans fil.

**Sur la protection des enfants :**

[www.saferinternet.fr](http://www.saferinternet.fr)  
[www.internetsanscrainte.fr](http://www.internetsanscrainte.fr)  
[www.netecoute.fr](http://www.netecoute.fr)  
[www.info-familles.netecoute.fr](http://www.info-familles.netecoute.fr)  
[www.e-enfance.org](http://www.e-enfance.org)

**Pour s'informer :**

[www.cnil.fr](http://www.cnil.fr)  
[www.securite-informatique.gouv.fr](http://www.securite-informatique.gouv.fr)  
[www.hadopi.fr](http://www.hadopi.fr)  
[www.hoaxbuster.com](http://www.hoaxbuster.com)  
[www.cnac-contrefacon.fr](http://www.cnac-contrefacon.fr)  
[www.netpublic.fr](http://www.netpublic.fr)

**Pour signaler les abus :**

[www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr)  
[www.pointdecontact.net](http://www.pointdecontact.net)

**Pour apprendre et découvrir :**

[www.panelparents.fr](http://www.panelparents.fr)  
[www.vinzetlou.net](http://www.vinzetlou.net)  
[www.pedagojeux.fr](http://www.pedagojeux.fr)  
[www.2025exmachina.net](http://www.2025exmachina.net)  
[www.2020energy.eu](http://www.2020energy.eu)  
<http://eduscol.education.fr>

**Sur les logiciels libres :**

[www.april.org](http://www.april.org)  
[www.framasoft.net](http://www.framasoft.net)