Les guides pratiques de l'Udaf de l'Essonne

Familles et numérique : Surfer et acheter en toute sécurité

Sommaire

I. Surfer en toute sécurité
    1. Définition
    2. Le paramétrage et la sécurité de l'ordinateur
    3. Les différents modes de connexion
    4. Mes données, mes traces
II. Acheter en toute sécurité
    1. Les précautions préalables
    2. Le contrat de vente
III. L'utilisation d'Internet au sein de la famille
    1. Les nouvelles façons de se connecter
    2. Les informations et les contenus sur internet
    3. Le contrôle parental
    4. L'utilité d'internet

Mes outils pratiques

Outil pratique 1 : Mes courriels et pièces jointes, mode d'emploi
Outil pratique 2 : Mes mots de passe, mode d'emploi
Outil pratique 3 : Mes sauvegardes, mode d'emploi
Outil pratique 4 : Mes téléchargements, mode d'emploi
Outil pratique 5 : Les logiciels libres
Outil pratique 6 : Mes lettres types

1 ère partie :

I. 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.

1. Définition

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

2. 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. S'ils permettent d'exécuter certains programmes dans le

navigateur 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[*].

A. 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.

B. 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 en réparant 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 automatiques 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.

---

[*] Se reporter à l'outil pratique : les gestionnaires de mots de passe

ZOOM sur les cookies, traceurs, ver et spam

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 de leur fournir un moyen de les refuser.
Le consentement a une durée de validité de 13 mois.

2. Spam :

C'est un courriel non sollicité par son destinataire et source d'une gène manifeste (pourriel). Le spam encombre les boites 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*.
Les pourriels peuvent prendre la forme de simple publicité.

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

3. Ver

* Pour plus d'informations : zoom sur les risques

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.

3. Les différents modes de connexion

A. Les techniques de connexion

Il existe trois 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 boitier, 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 ;

* Pour plus d'information : Zoom sur les structures et les lieux ressources
* Pour plus d'information : « les mots de passes mode d'emploi » page 1

- 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. Les appareils (PC ou PDA) connectés à un réseau sans fil disposent d'une carte réseau munie d'une adresse spécifique : l'adresse MAC ;
- En configurant les machines Wifi en fonction des changements effectués (mots de passe, nom du réseau, clé de cryptage).

B. Les outils de connexion

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

C. Les lieux de connexion

- Les 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 ou et de ne pas faire d'achats en ligne à partir d'une connexion dans un lieu public.
- Les 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.

4. Mes données, mes traces

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.
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.
Il est 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.

A. Les réseaux sociaux

L'utilisation des réseaux comportent des risques, notamment celui de perdre la maîtrise de son identité numérique, puisqu'un nombre très important d'informations personnelles y sont disponibles. 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 maitriser 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.

B. 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 répondre à ces courriels et les supprimer.

3. Le vol d'identité
L'usurpation d'identité consiste à utiliser des données personnelles d'un individu, à son insu.

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*.

*Se reporter à l'outil pratique : Mes lettres types

2ème partie

II. 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

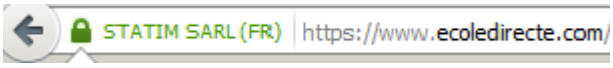
Attention : les recommandations suivantes ne sont valables que pour les sites marchands français, les sites étrangers ne répondant pas à la législation française. Il est donc essentiel de vérifier, avant tout achat, dans la rubrique des mentions légales, l'adresse du siège social et le numéro de téléphone,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

1. Les précautions préalables à l'achat en ligne

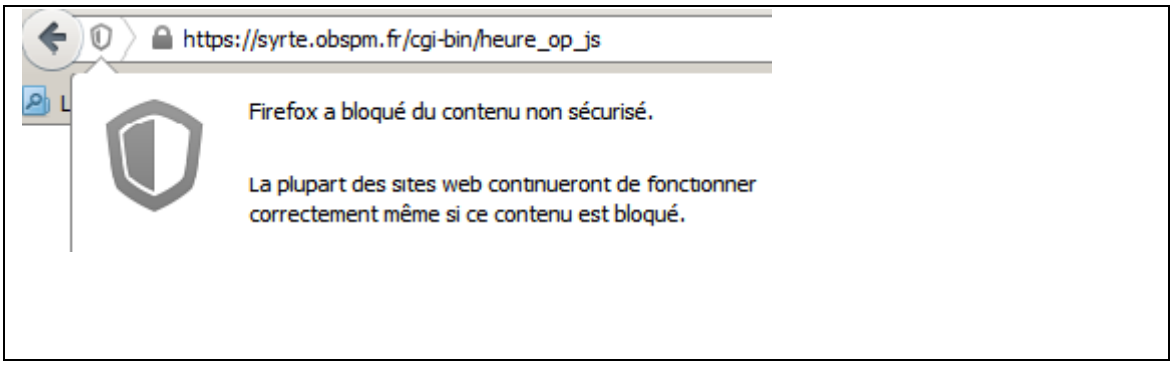
ZOOM sur la sécurité des sites marchands

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

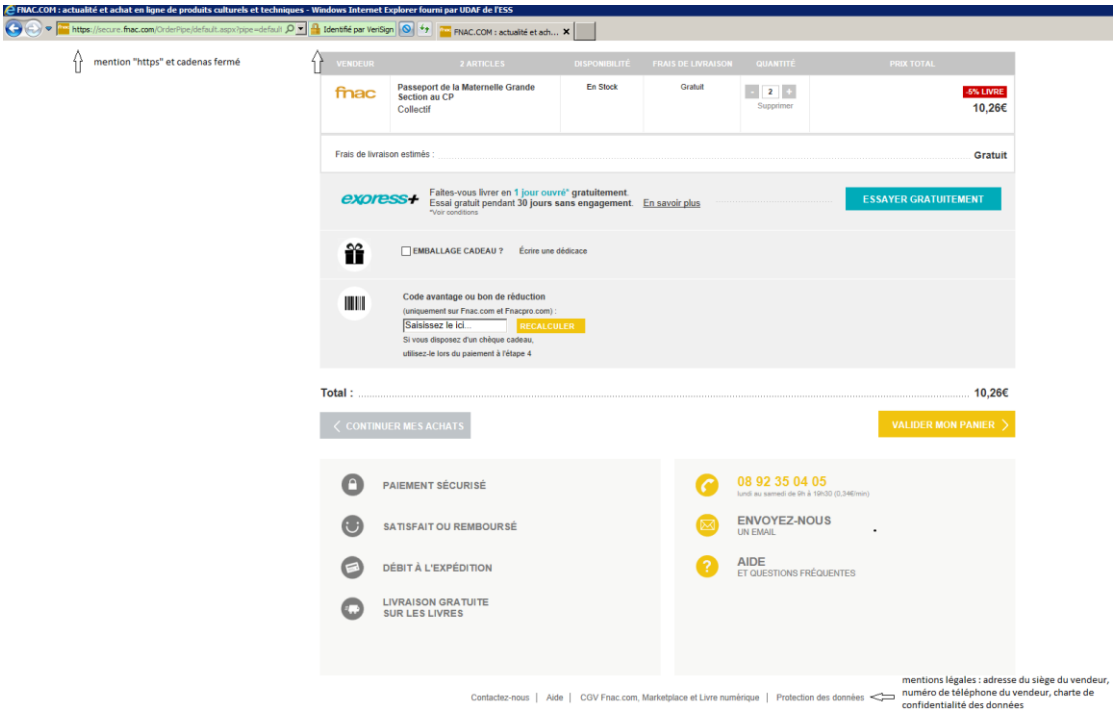
Cadenas fermé : lorsque la page est entièrement sécurisée



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



Il est important de vérifier :



- 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 boite 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. Dans ce cas, il faut garder à l'esprit que le consentement du consommateur doit être obligatoirement demandé.

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

2. Le contrat de vente

La commande doit être présentée en trois étapes :

- Visualisation du détail de la commande (le prix doit être TTC et doit être exprimé en euros) ;
- Correction d'éventuelles erreurs ;
- 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 consommateur[†].

A. 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.

[†] Pour plus d'informations : Zoom sur les structures et les sites ressources.

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.

B. 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.

C. 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 a 70 jours à partir de la date de l'opération contestée pour déposer une réclamation. Dans ce cas, c'est le vendeur qui assume le coût de vente.
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.

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 particulier, il est essentiel d'attendre le contrat de location avant de verser un acompte.

3ème partie :

III. L'utilisation d'Internet au sein de la 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.

1. 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 empêche 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 (jusqu'à trois ans d'emprisonnement et 300 000 euros d'amende 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 ou le cyber-bullying[‡]), 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.

2. Les informations et les contenus sur Internet

A. Apprendre à faire le tri dans les informations

Sur internet, des d'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 écrits. L'auteur peut influencer le point de vue du lecteur ;
- Éviter les sites personnels ;
- Vérifier la date de publication de l'information.

B. 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. Dans tous les cas et pour tous les contenus, l'accord de l'auteur est nécessaire.

Pour trouver des images afin d'alimenter un devoir ou pour toute autre utilisation, l'image choisie doit être libre de droit. C'est-à dire que l'auteur de l'image autorise quiconque à la reproduire et à la diffuser. Parfois, son auteur peut autoriser à reproduire, diffuser et modifier son œuvre, sous les mêmes

[‡] Pour plus d'information : se reporter à l'outil pratique : les définitions

conditions de distribution que l'œuvre d'origine. Cependant, l'auteur de l'image peut apporter certaines restrictions comme l'obligation pour l'utilisateur d'indiquer l'auteur de l'image choisie (paternité de l'image), de ne pas en faire la commercialisation, etc

Comment repérer les images qui sont libres de droit ?

- Rechercher les images sous licences « Creative Commons ». Celles-ci fournissent un cadre d'utilisation très clair, qui permet d'éviter tout risque d'infraction au droit d'auteur.
- Rechercher les images tombées dans le domaine public. Ces images sont commercialisables librement. Dans google ou Wikimedia Commons, taper les mots clés souhaités ainsi que « public domain » pour n'obtenir que les images correspondantes.
- Vérifier, dans tous les cas, les conditions d'utilisation des photos sur la page web de destination pour éviter tout risque d'infraction au droit d'auteur.

Où trouver les images libres de droits :

- Wikimedia Commons : Cette base de données multimédia centralise des millions de médias libres, dont une grande quantité d'oeuvres visuelles accessibles via un moteur de recherche. Ces photos sont regroupées ensuite par thèmes selon les thèmes des mots-clés utilisés.
- Search.creativecommons.org : ce site regroupe différents moteurs de recherche et plateformes d'hébergement de photos sous licences Creative Commons.
- Flickr.com/creativecommons : La célèbre plateforme d'hébergement de photos regroupe toutes les oeuvres hébergées par type de licence Creative Commons.

3. Le contrôle parental

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

A. 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 sur les téléphones portables connectés en wifi.

B. Les bons réflexes à transmettre aux enfants

Parce que le contrôle parental ne suffit pas et qu'à termes 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 réélle ;
- Paramétrer ensemble les critères de confidentialité sur les réseaux sociaux notamment.

4. L'utilité d'internet

A. 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 en ligne, des services en ligne tels que la consultation des comptes, ou encore de bénéficier de la possibilité de procéder à des virements.

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.

B. 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, 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, d'informations, qui leur permettent de communiquer entre eux ou de créer.

Zoom sur les structures et les sites ressources

Sur la protection des enfants :
www.e-enfance.org
www.saferinternet.fr
www.internetsanscrainte.fr
www.actioninnoncence.org
www.netecoute.fr
www.info-famille.netecoute.fr

Pour s'informer :
www.cnil.fr
www.securite-informatique.gouv.fr
www.hadopi.fr

Pour signaler les abus :
www.internet-signalement.gouv.fr
www.pointdecontact.net
sosbenjamin
www.mineurs.fr

Pour apprendre et découvrir :
www.vinzetlou.net
www.kidinet.fr
www.pedagojeux.fr
www.2025exmachina.net
www.educnet.education.fr

Page d’insertion outils pratiques

4ème de couverture

Edito Udaf

Logo(s)