Internet
Bons usages et astuces

LES BONS USAGES D'INTERNET

Quelques conseils aux parents !

Les écrans sont aujourd'hui **incontournables** dans nos quotidiens et leur utilisation peut avoir de nombreux avantages tels que l'accès à une information plurielle et large, l'accès à la culture ou encore le maintien des relations sociales. Toutefois, cela est conditionné à un **usage raisonné** par les utilisateurs et ce, dès le plus jeune âge. Pourtant, Internet est le seul risque auquel les parents n'ont jamais été exposés étant enfant ! Ils ont ainsi un **rôle fondamental** à jouer dans l'accompagnement de leurs enfants dans l'univers numérique afin de leur donner toutes les clés d'une expérience en ligne **sûre et maîtrisée** : d'où la nécessité d'accompagner les enfants avant de les laisser circuler seuls sur le web.

Partager les mots de passe et pseudo de ses enfants

Vous devez aider votre enfant à construire des **pseudos et mots de passe sûrs**.

Il est important de **connaître** les pseudos et mots de passe de votre enfant. Un pseudo fiable ne doit donner **aucune indication** sur le nom, le prénom, la localisation géographique ou encore l'âge de votre enfant. Un mot de passe fiable doit comporter des **chiffres et des lettres** en évitant les mots de passe évidents comme ceux reprenant le prénom ou la date de naissance de votre enfant. Par exemple : « ZoeMartin10ansAnnecy » est un mauvais pseudo... En revanche, « skyDe4@l, zorglub0) ou De5=straac », sont de bons pseudos car ils ne révèlent rien sur l'identité, l'âge, le nom ou la localisation géographique. Si vous prenez les premières lettres des mots d'une phrase que votre enfant connaît par cœur comme « j'aime les pains au chocolat » et que vous y ajoutez un chiffre, cela donne JALPAC3, un bon mot de passe.

De la même façon que vous savez où votre enfant va dans la rue, vous devez savoir **où il va sur Internet**. Il en va de même pour ses amis : vous connaissez ses amis dans la vie, vous devez **connaître ses amis sur Internet**. Vous devez entretenir le **dialogue** avec votre enfant pour le protéger au mieux.

Mettre en place le contrôle parental

Il permet de **protéger votre enfant** de certains contenus et images qui ne sont pas appropriés à son âge et pourraient le choquer. Le contrôle parental est indispensable pour une **bonne utilisation d'Internet** par votre enfant. Il permet également de vous protéger de sites qui pourraient contaminer votre ordinateur par le biais de virus.

Toutefois le contrôle parental ne suffit pas et ne doit pas vous empêcher de **surveiller la navigation** de votre enfant. Il faut voir le contrôle parental comme une alarme de piscine. Ce n'est pas parce que la piscine est équipée d'une alarme qu'il ne faut pas surveiller les enfants au bord de l'eau !

Les ordinateurs, tablettes et portables : dans une pièce commune !

Pour vous permettre de **surveiller la navigation** de votre enfant plus sereinement, il est fortement recommandé d'installer l'ordinateur ou la tablette numérique (mais aussi la télévision) dans une pièce commune et de **limiter son utilisation** à cette pièce.

Cela vous permettra de toujours garder un œil sur ce que fait votre enfant et il sera plus facile pour lui de vous interpeller s'il a des questions, des remarques. Il est important de **maintenir un dialogue constant** pour que votre enfant n'ait pas peur de vous parler.

Incitez-le à faire de petites pauses régulières afin de rester maître de son attention.

Apprenez-lui à **éteindre les écrans** dans la pièce dans laquelle il fait ses devoirs et de les retirer de sa chambre quand il va se coucher.

Respecter la classification par âge

Le **PEGI** (« Pan European Game Information »), est un système destiné à informer les consommateurs et notamment les parents de l'**âge minimum** souhaitable pour jouer à un **jeu vidéo**, selon des caractéristiques bien définies, tels que le niveau de violence verbale, de violence physique, ou encore le caractère effrayant du jeu vidéo ou du film... De même, la **signalétique jeunesse** est l'outil clé du dispositif créé par le CSA au service de la protection de la jeunesse et des mineurs concernant **la télévision.**

Il est indispensable de **respecter ces classifications pour protéger vos enfants** d'images ou de propos qui pourraient être choquants.

Développer l'esprit critique des enfants

Pour que votre enfant devienne un **utilisateur responsable et conscient** d'Internet, il est important de développer son **sens critique**.

Incitez-le à **se poser des questions** sur les résultats de ses recherches, sur les personnes ou sites qui souhaitent entrer en contact avec lui, sur les images qu'il voit et les informations qu'il reçoit.

Plus tôt votre enfant développera son sens critique, plus il sera **protégé** et protégera **sa vie privée et la vôtre** lors de ses utilisations d'Internet.

Une ligne à votre écoute

Si votre enfant a besoin d'une **aide psychologique** en cas de confrontation à des problèmes liés à Internet (dépendance, harcèlement / cyber harcèlement...), vous pouvez contacter **Net Ecoute**, une ligne d'assistance téléphonique qui a été mise en place par des spécialistes de l'enfance et d'Internet et des psychologues : **3018** Ligne gratuite ouverte du lundi au vendredi de 9h à 20h et le samedi de 9h à 18h. Par téléphone, chat, Skype et email.

LE CONTRÔLE PARENTAL

Quelques faits :

- **Une exposition précoce et de plus en plus massive des enfants aux écrans :**
  Avec une multiplicité des écrans au sein des foyers (télévision, ordinateur, smartphone, tablette, console de jeux, etc.), l'exposition précoce des enfants aux écrans s'est amplifiée. Celle-ci peut **nuire au bon développement de l'enfant.** Il convient donc d'éviter l'exposition des enfants de moins de trois ans aux écrans et de veiller à l'**usage raisonnable** des écrans des plus grands.
- **Des répercussions possibles sur la santé des enfants :**
  La surexposition aux écrans ou leur gestion inappropriée peut entraîner des **risques et des effets sur la santé des enfants** tels que le sommeil, la vision, le développement cognitif ou encore le poids. Par exemple, le temps passé devant une télévision peut être associé à une augmentation des prises alimentaires et à une altération du sommeil.
- **Le besoin d'accompagnement des enfants par les parents :**
  Les écrans sont aujourd'hui incontournables dans nos quotidiens et leur utilisation peut avoir de **nombreux avantages** tels que l'accès à une information plurielle et large, l'accès à la culture ou encore le maintien des relations sociales. Toutefois, cela est **conditionné à un usage raisonné** par les utilisateurs et ce, dès le plus jeune âge. Les parents ont ainsi un rôle fondamental à jouer dans l'accompagnement de leurs enfants dans l'univers numérique.

Le contrôle parental pour quoi faire ?

- Pour protéger au mieux votre enfant, il est primordial d'installer un contrôle parental sur **l'ensemble des équipements** qu'il utilise, y compris les vôtres et de paramétrer l'ensemble des réseaux sociaux, plateformes en ligne, sites et applications qu'il utilise.
- Pour sensibiliser les jeunes aux bons usages et bonnes pratiques du numérique et ainsi leur donner toutes les clés d'une expérience en ligne **sûre, émancipatrice et maîtrisée.**
- En tant que parents responsables, c'est à nous de veiller à ce que nos enfants utilisent ces appareils **à bon escient**, en nous assurant qu'ils n'abusent pas de leur accès et que le contenu qu'ils regardent et avec lequel ils interagissent est **adapté à leur âge**.
- Le contrôle parental est avant tout un outil, il n'est pas infaillible et **ne se substitue pas** à la vigilance, à l'écoute et au **dialogue avec votre enfant.**
- Maîtriser le temps d'écran, connaître le comportement de votre enfant, outil par outil, afin de **l'accompagner** dans une meilleure gestion de sa consommation et le prémunir contre des comportements qui pourraient être risqués.

Comment le mettre en place ?

Nous vous conseillons d'aller sur le site jeprotegemonenfant.gouv.fr, plateforme d'information et d'accompagnement à la parentalité numérique pour un usage raisonné des écrans par les enfants.

Vous y trouverez les informations vous permettant d'**installer et configurer le contrôle parental** sur vos appareils et consoles, de paramétrer le filtrage de certains contenus sur les réseaux sociaux ou encore d'activer un outil de limitation de temps d'écran, filtrer les accès et les protéger des contenus non appropriés.

Tous les équipements numériques que vous utilisez peuvent être configurés : Smartphone, tablette, ordinateur, console de jeux... Ces outils sont disponibles sur l'ensemble des supports et équipements ainsi que sur les sites et applications utilisés par votre enfant. Ils peuvent être adaptés en fonction de son âge.

N'oubliez cependant pas que **la communication et l'exemple** sont les deux piliers d'une **utilisation saine, comprise et acceptée par tous**.

Sur vos téléphones, vous pouvez vous rendre compte de votre consommation, et définir des objectifs. Ces fonctionnalités vous permettent d'accéder à des rapports en temps réel indiquant le temps que vous passez sur votre portable, par application.

Vous pouvez également définir des limites pour les aspects que vous souhaitez gérer.

Ainsi, sur Android, l'application **"Bien être numérique"** vous permet de savoir combien de temps vous avez passé sur telle ou telle application, mettre en place un contrôle parental, un mode "chut" ou "sommeil".

Pour les Iphone, il s'agit de la fonctionnalité **"Temps d'écran".**

Celles-ci vous permettront de **trouver l'équilibre** dans votre consommation numérique, pour vous et votre famille.

Les applications de contrôle parental

Outre les fonctionnalités offertes par vos fournisseurs d'accès à Internet, plusieurs applications existent pour un contrôle parental sur vos équipements.

Parmis les plus connues, **Family Link** vous permet, à partir d'un compte google que vous pouvez créer avec votre adresse mail actuelle, d'associer gratuitement l'appareil de votre enfant au vôtre, afin que vous puissiez **définir des règles de vie numérique de base**, fixer des temps d'utilisation, gérer les applications et les sites Web que votre enfant utilise.

D'autres applications gratuites ou payantes sont aussi disponibles :

Famisafe, Kidlogger, QuStodio, Norton Family, Family Keeper, Net Nanny, Kaspersky safe Kids, etc...

Suivant les fonctionnalités désirées et votre budget, vous trouverez facilement l'application de contrôle parental **qui convient à votre famille** !

LES RÉSEAUX SOCIAUX

Quelques règles de base pour une utilisation sécurisée

Pour les jeunes, les réseaux sociaux sont avant tout un **moyen de communication et de divertissement**.
S'ils en sont si friands, c'est parce que les réseaux sociaux répondent à leurs besoins d'autonomie, d'individualisation, d'émancipation…
Leurs présences numériques leur permettent de se retrouver, de développer des relations, d'échanger sur leurs expériences, leurs sentiments et leurs questionnements et ce, **en dehors de la sphère des adultes.**
A un âge où ils construisent leur personnalité, c'est un **territoire d'expression libre** où ils peuvent se confronter aux autres tout en renforçant leur sentiment d'appartenance à un groupe.

Pour un usage sécurisé des Réseaux Sociaux, il faut :

- Restreindre ses comptes sur les réseaux sociaux (les paramétrer)
- Ajouter uniquement les personnes que l'on connaît dans la "vraie vie"
- Ne pas télécharger de photos d'autres personnes sur un réseau social sans qu'elles ne soient au courant et d'accord.
- Avertir immédiatement un adulte si quelqu'un partage un contenu inapproprié.
- Ne pas insulter, menacer ou se moquer de qui que ce soit.
- Discuter avec ses enfants pour qu'ils soient conscients des dangers

Prendre garde et faire preuve de vigilance

Sur les réseaux sociaux, on a parfois envie d'avoir beaucoup d'«amis », car ça donne l'impression d'être populaire. Mais il vaut mieux n'accepter que les personnes que l'on connaît vraiment, et faire attention à mettre son **compte en privé** pour éviter que n'importe qui voit ce qu'on publie.

Maîtriser ses publications

Les réseaux sociaux permettent de communiquer auprès d'une grande audience que vous ne pourrez jamais complètement maîtriser. Même dans un cercle que l'on pense restreint, vos publications peuvent vous échapper et être rediffusées ou interprétées au-delà de ce que vous envisagiez. Ne diffusez **pas d'informations personnelles** ou sensibles qui pourraient être utilisées pour vous nuire.

Faire attention à qui vous parlez

Sur les réseaux sociaux, il existe ce qu'on appelle des cybercriminels, ce sont des personnes qui les utilisent notamment pour commettre des escroqueries et voler des informations personnelles ou professionnelles. **Soyez vigilants**, car à leur insu, vos amis ou contacts peuvent également vous envoyer ou partager des contenus malveillants, surtout s'ils se sont fait pirater leurs comptes sans le savoir.

Les avantages des Réseaux Sociaux

Il participent à démocratiser l'éducation

Il y a encore quelques années, seul un groupe de personnes bien spécifique avait accès à l'enseignement le plus qualitatif. Aujourd'hui, avec les différents médias sociaux, il est possible d'**accéder à toutes les informations** possibles et imaginables de façon totalement gratuite.

Ils permettent de rester informer sur la situation mondiale

Les réseaux sociaux ont participé à l'accélération de la diffusion de l'information. Ainsi, sur son fil d'actualité Twitter, Instagram ou Facebook, on peut découvrir des nouvelles qui arrivent de l'autre bout du globe **en temps réel**. On peut notamment citer l'exemple récent du Covid-19 où les lanceurs d'alertes chinois ont permis d'informer le monde entier de la situation à Wuhan à l'aube de la crise sanitaire.

Rester connecté avec ses proches

Dans un contexte où voir sa famille et ses amis en face-à-face est plus compliqué que jamais, les réseaux sociaux se proposent comme une alternative afin de **maintenir le lien social** entre personnes grâce aux outils de communication instantanée, aux jeux et au partage de médias que les plateformes proposent.

Ils ouvrent la porte à de nombreuses opportunités

Internet et les réseaux sociaux ont apporté leur lot d'opportunités. On peut citer la **création** de nouveaux emplois comme le métier d'influenceur ou de webmarketer, mais aussi la possibilité de **découvrir** des activités et des connaissances inconnues, ou de **toucher des personnes** qui étaient jusqu'alors hors de portée (stars, personnes influentes, politiciens...).

Les réseaux sociaux aident à créer un sens de communauté

Dans un monde globalisé où il existe des tas d'individus aux personnalités et aux intérêts différents, les réseaux sociaux permettent d'unifier certains groupes qui **partagent des valeurs communes**. Ainsi, des personnes isolées du fait de leur sexualité, religion, milieu social, passion, peuvent entrer en contact avec des individus qui leur ressemblent et retrouver le sentiment d'**appartenir à une communauté**.

Une prise de conscience collective

Les réseaux sociaux sont des outils puissants qui permettent de **mettre en évidence des problèmes fondamentaux de notre société**. Ce sont les fers de lance qui sensibilisent les populations aux sujets majeurs de notre temps tels que le réchauffement climatique, les inégalités sociales, les guerres et autres conflits géopolitiques dans le monde.

Les risques des Réseaux Sociaux

Le cyberharcèlement

Le cyberharcèlement se définit comme un **harcèlement s'effectuant via internet** (sur un réseau social, un forum, un jeu vidéo, un blog...). Il consiste à tenir des propos ou avoir des comportements répétés ayant pour but ou effet une dégradation des conditions de vie de la victime. Le cyberharcèlement peut prendre plusieurs formes mais la plus commune d'entre elles est notamment les **commentaires** (sur les publications, ou même sur les messages privés). Le harcèlement en ligne est puni par la loi, que les échanges soient publics ou privés (messagerie instantanée inclue). Cette violence commise derrière un écran, est particulièrement dangereuse puisqu'elle est **immédiate, rapide et très souvent virale.**

Les cyberprédateurs

Les prédateurs sexuels et autres prédateurs en tout genre ont de nos jours la possibilité de traquer les enfants sur les réseaux sociaux en **abusant** de leur confiance et en profitant de leur innocence. Tout comme les cyberharceleurs, leurs terrains d'actions sont notamment les divers réseaux sociaux. Pour protéger vos enfants contre ces individus mal intentionnés, la meilleure méthode est de **parler avec eux** afin de leur faire **prendre conscience de ce risque.**

Les arnaques

Les réseaux sociaux constituent le lieu idéal pour les gens mal intentionnés. Ces derniers y diffusent des contenus recelant des liens corrompus dans la seule intention d'arnaquer les internautes. Vous devez donc prendre le temps d'expliquer correctement à vos enfants les risques qu'ils encourent sur les réseaux sociaux et les prévenir sur les fraudes en ligne. Apprenez-leur aussi les **choses à faire ou à ne pas faire** pour éviter toutes formes d'arnaque.

Le risque d'addiction

Les réseaux sociaux ont un caractère addictif, et les enfants peuvent y être très vulnérables. En effet, lorsqu'une personne découvre fraîchement le contact social, les likes, les demandes d'amis, bref la vie sur les réseaux sociaux, elle a tendance à y passer beaucoup de temps. Pour prévenir cela, **définissez un temps de connexion et limitez l'accès à internet** de vos enfants. Là encore, la communication est le point le plus important pour qu'ils comprennent les risques qu'ils encourent.

La publication d'informations privées

Les enfants ne comprenant pas encore la notion de **limites sociales,** il est possible qu'ils publient des informations personnelles sur les réseaux sociaux. Rappelez donc à vos enfants que si vous pouvez voir ce qu'ils publient, **tout le monde peut voir aussi**. Discutez avec eux des limites sociales et de ce qu'ils peuvent publier ou non.

LA SÉCURITÉ SUR INTERNET

Quelques règles de base pour une utilisation sécurisée d'internet :

- Ne jamais utiliser son nom et sa date de naissance dans un mot de passe
- Ne jamais installer d'applications sans l'autorisation d'un adulte
- Ne pas partager les mots de passe en dehors de la cellule familiale
- Ajouter uniquement les personnes que l'on connaît sur les réseaux sociaux
- Ne pas partager de photos d'autres personnes sur un réseau social sans qu'elles ne soient au courant et d'accord.
- Avertir immédiatement un adulte si quelqu'un partage un contenu inapproprié.
- Ne pas insulter, menacer ou se moquer de qui que ce soit sur internet.
- Utilisez un moteur de recherche adapté (Qwant, Qwant Junior, Kiddle...)

Prendre garde et faire preuve de vigilance

Comment se comporter de manière responsable ?

Ne croyez pas tout ce que l'on raconte sur la toile et soyez méfiants lorsque vous naviguez sur Internet. Par ailleurs, **protégez** votre ordinateur et vos dispositifs mobiles avec un mot de passe sécurisé.
L'utilisateur représente très souvent le premier facteur de risque.
À vous donc de faire preuve de bon sens !
Par exemple : dans les cas d'une attaque de phishing par mail ou par téléphone, des escrocs peuvent se faire passer pour votre banque et essayer de vous attirer sur un site contrefait qui ressemble presque parfaitement à celui de votre banque. Si vous tombez dans le panneau et que vous communiquez vos codes d'accès, les malfaiteurs pourront dévaliser votre compte en toute tranquillité.

N'oubliez jamais que **votre banque ne vous demandera jamais vos données d'accès** à son service de banque en ligne. Faites donc preuve du juste degré de méfiance !

Comme vous devez être conscient des dangers des e-mails d'hameçonnage (phishing) et de l'importance de protéger vos informations personnelles, **soyez vigilants**, ne cliquez sur les liens suspects et n'ouvrez pas les pièces jointes reçues à partir d'adresses e-mail inconnues ou que vous trouveriez "bizarres".

Vous ne protégerez ainsi pas seulement les informations privées du propriétaire du compte, mais vous vous assurerez qu'aucune malveillance n'affecte un appareil que d'autres membres de la famille pourraient utiliser.

Une utilisation réfléchie des mots de passe

Un mot de passe simple et court n'offre pas une protection suffisante dans la mesure où il pourrait être facilement deviné. Évitez donc les noms, prénoms d'enfants ou d'animaux, les mots pouvant figurer dans un dictionnaire d'une langue connue, les combinaisons de touches voisines (ex.: « qsdfg » ou « 45678 »), de même que les dates de naissance.

L'idéal est de créer une combinaison arbitraire d'au moins 10 caractères contenant à la fois des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. N'utilisez pas partout le même mot de passe. Au contraire, il convient d'en trouver un différent pour chaque compte et de **ne jamais les donner à qui que ce soit**. Mémorisez vos mots de passe ou conservez-les sous forme écrite dans un lieu sûr.

Créer un mot de passe sûr n'est pas si difficile que ça !

- Choisissez une **phrase facile à mémoriser** et élaborez votre mot de passe en prenant la première lettre de chaque mot et en incluant des chiffres et des caractères spéciaux : « Ma fille Tamara fête son anniversaire le 19 janvier ! ». Vous obtenez alors une chaîne de caractères apparemment arbitraire mais facile à mémoriser : « MfTfsal19j! »
- Choisissez des mots de passe de **10 caractères au moins**. Ils doivent être composés d'une combinaison arbitraire de chiffres, de lettres majuscules et minuscules, et de caractères spéciaux.
- Ne **communiquez à personne** vos mots de passe et conservez-les toujours en lieu sûr, sous forme chiffrée si possible.
- N'enregistrez pas les mots de passe que vous utilisez pour accéder à des sites protégés dans votre navigateur. Les navigateurs n'assurent généralement pas un niveau de sécurité suffisant pour la gestion de ces mots de passe.

Principaux conseils à suivre

- Soyez **toujours prudent** lorsque vous surfez sur Internet et réfléchissez bien avant de communiquer vos données personnelles.
- Les banques, les opérateurs téléphoniques ou autres fournisseurs de service **ne vous demanderont jamais** (que ce soit par email ou par téléphone) de leur communiquer votre mot de passe, ni de le modifier.
- Lorsque vous utilisez vos dispositifs mobiles, vous devez appliquer **les mêmes mesures** de précaution que celles que vous observez normalement sur votre ordinateur.

LES LOGICIELS LIBRES & OPEN SOURCE

Qu'est-ce que c'est ?

Le marché informatique est dominé en grande partie par les logiciels propriétaires. Ces derniers sont certes efficaces, mais payants et leur code est jalousement gardé par leurs concepteurs. La solution alternative réside dans les **logiciels libres et open source.** Ceux-ci prônent une **philosophie axée sur le partage et le soutien de la communauté**.
Le logiciel libre, selon son initiateur, est un mouvement social qui repose sur les principes de Liberté, Egalité, Fraternité ; l'open source quant à lui s'attache aux avantages d'une méthode de développement, aux travers de la réutilisation du code source. (En informatique, le code source est un texte qui présente les instructions composant un programme sous une forme lisible, telles qu'elles ont été écrites dans un langage de programmation.) Distribué selon une licence libre, un logiciel libre est open source. C'est-à-dire qu'il peut être librement utilisé, étudié, modifié, copié, amélioré et redistribué.

Les avantages du logiciel libre :

Dans un monde où la plupart des sociétés s'attachent à protéger la propriété intellectuelle à tout prix, le logiciel libre est une bouffée d'air frais. Synonyme de bien commun, l'esprit du logiciel libre appuie cette volonté de **rendre le progrès et la connaissance accessible à tous.**

Il est indépendant

Là où un logiciel propriétaire n'appartient qu'à un seul, le logiciel libre est l**a propriété de tous**. Par exemple, les mots clefs tapés dans la barre de recherche Google Maps sont la propriété de Google tandis que les données transmises à OpenStreetMap appartiennent à la communauté.

Il est de meilleure qualité

Un logiciel libre peut être soumis à l'étude, la critique ou la correction de plusieurs contributeurs. Ce qui lui confère une **réelle fiabilité et réactivité**.
Permettant la contribution de tous, un logiciel libre bénéficie des connaissances techniques et du savoir-faire d'un écosystème de prestataires divers. Plus il y a de participants, plus la qualité du logiciel s'améliore.

Il est gratuit ou moins cher

Fruit d'un **développement communautaire**, un logiciel libre n'est pas forcément gratuit mais présente un coût avantageux. L'utilisateur ne doit pas payer le coût de la licence.
La partie payante du logiciel concerne le coût du service, le développement ou la maintenance.

Il est éthique

Un logiciel libre **repose sur des valeurs humaines**. Refusant l'objectif commercial, il propose une autre approche de l'économie. Ainsi, il se différencie du système de licence commerciale qui empêche toute diffusion et réappropriation du logiciel.

Il est plus sécurisé

Un logiciel libre est davantage sécurisé. Le code source peut être analysé et retravaillé par le plus grand nombre. Tout utilisateur a donc les moyens de corriger les erreurs éventuelles qu'il aurait détectées. Les **failles sont ainsi réparées** plus rapidement que pour un logiciel propriétaire.

Il est plus durable

N'ayant pas de concurrence, le logiciel libre s'avère être une solution plus pérenne. **Fondé sur les principes de collaboration et d'entraide**, le logiciel libre s'offre de meilleures chances de survie. Ceux qui dans le cas d'un logiciel propriétaire deviendraient des concurrents sont ici de potentiels collaborateurs.

Exemples de différents logiciels libres accessibles pour tous :

Des navigateurs : Libres, gratuits et rapides, disponibles pour tous les supports : **Firefox, Brave** ou encore **Tor.**

Des suites bureautiques : Elles comportent généralement un traitement de texte, un tableur, un logiciel de présentation, un outil de dessin. Les principales sont **Libre Office** et **Open Office**

Des logiciels PAO, MAO, lecteurs multimédia…

Pour monter vos vidéos, enregistrer du son, ou lire la plupart des formats audio et vidéo : **Shotcut, Audacity** ou **VLC**.

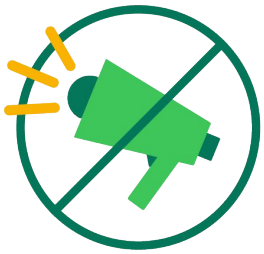
Pour une alternative à photoshop ou pour créer des documents à publier avec une qualité pro, **GIMP**, **Scribus ou Krita**

Pour des dessins vectoriel ou de l'animation, **Inkscape** ou **Blender**

Des outils…

Pour la gestion des pdf : **PDFSam** ou encore **PDF Creator**, **7-Zip** permettent de compresser vos dossiers et vos fichiers afin qu'ils utilisent moins d'espace sur votre disque dur.

Vous le voyez, les logiciels libres n'ont **rien à envier aux logiciels propriétaires** !
Et pour compléter ce petit tour d'horizon, vous en trouverez une liste non exhaustive ici : **http://www.pack-logiciels-libres.fr/**



LES FAKE NEWS

Une Fake News, qu'est-ce que c'est ?

Une fake news est une **information fausse** diffusée (de façon inconsciente ou sciemment) **pour influencer une opinion**, tromper un auditoire, manipuler le public.

On dit aussi *infox, intox, rumeur*. C'est la diffusion à grande échelle d'un canular, d'une fausse histoire ou d'une information délibérément erronée, pour créer de la confusion, influencer l'opinion publique, tromper les internautes...

Si les fake news ont toujours existé, le phénomène s'est accentué avec l'omniprésence d'Internet et s'est clairement accéléré ces dernières années.

Ce qui change avec Internet, c'est la **rapidité de diffusion et la qualité de ces fake news**.

Dans certains cas, il s'agit d'une véritable arme de communication qui peut déstabiliser et orienter l'opinion.

Il faut donc toujours **vérifier les infos** et surtout **ne pas partager** si on n'est pas absolument sûr !

Le problème, c'est que **les fausses informations sont partout** et il n'est pas évident de les repérer. Youtube, Facebook, SnapChat ne sont pas épargnés ; pire, ils sont une vitrine de choix pour la diffusion en masse de fake news.

Pointés du doigt un temps pour leur manque d'investissement dans la lutte contre les infox, les géants du web ont lancé une contre-attaque en pénalisant les comptes, médias, individus propageant de fausses informations non vérifiées.

De leur côté, les institutions, les médias d'informations, les associations, etc, ont **mis en place des dispositifs pour vérifier les rumeurs**, données sans source, et autres informations douteuses circulant en ligne.

Comment évaluer la qualité et la pertinence d'une information et discerner le vrai du faux ? Voici quelques questions à se poser au quotidien :

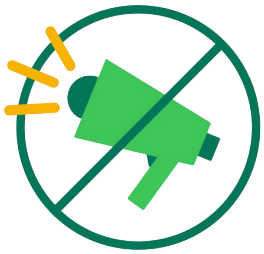
Qui est l'auteur de l'information ?

La première chose à faire avant de partager une information, c'est de se demander **qui l'a mise en ligne**. Le fait qu'un compte soit certifié ou détenu par une personnalité n'indique pas nécessairement que l'image soit vraie. En revanche, si elle a été publiée par un compte créé une heure avant, vous pouvez vraiment douter... Il est important de déterminer la **légitimité de l'auteur** : est-il un expert ou non sur le sujet ? Certains sites proposent même d'accéder, via un lien hypertexte, à sa biographie et à l'ensemble de ses publications.

Quel est l'objectif de l'auteur ?

L'auteur peut **relater des faits** ou **exprimer son opinion** : ce n'est pas la même chose.

Une Fake News a forcément une intention malveillante...



Quelle est la nature du site et de son éditeur ?
Un blog, un site institutionnel, un média en ligne, un réseau social... la nature d'un site est aussi diverse que variée et peut apprendre beaucoup sur la **qualité d'une information**. C'est aussi le cas pour l'éditeur du site qui peut être un média détenu par un groupe français ou étranger, un parti politique, une entreprise, une association, un particulier...

Quels sont les objectifs du site ?
Un site peut avoir pour objectif de vendre, d'informer, de militer, de convaincre, de manipuler, de faire peur ou encore de faire le buzz.
En fonction de l'objectif du site, l'**information n'a pas la même pertinence**.

Comment se présente le site ?
La structure, l'ergonomie, la clarté de la langue, le type de publicités... la présentation d'un site est parfois **révélatrice de la crédibilité** des informations qu'on y trouve.

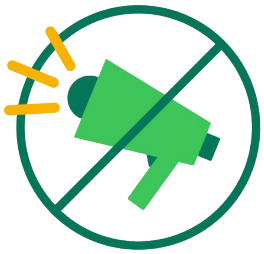
D'où provient l'information ?
Les **sources d'une information sont primordiales** pour déterminer sa crédibilité. L'origine d'un chiffre ou d'une citation, quand elle est mentionnée, permet au lecteur de s'y référer directement. Certains sites proposent des liens hypertextes renvoyant vers les sites sources.

L'information a-t-elle été publiée sur d'autres sites ?
Il est important de **comparer et de croiser les sources.** Cela permet de voir si l'information est présente sur d'autres plateformes et de voir comment elle y est traitée.

De quand date l'information ?
Il est important de savoir **à quel moment les faits relatés se sont produits**. Par exemple, certaines fausses informations s'appuient sur des images prises dans des contextes et à des moments différents pour commenter un sujet d'actualité. Les légendes sous les images, la date de publication d'un article, les métadonnées sont susceptibles d'apporter de **précieux renseignements**.

L'information présente-t-elle des détails incohérents ?
Par exemple, lorsque l'image ne correspond pas à la légende qui l'accompagne, cela doit éveiller les **soupçons sur la véracité de l'information**.

Que disent les commentaires ?
Parce qu'ils soulignent parfois l'incohérence d'une information, les commentaires sont utiles pour **jauger la crédibilité** des informations avancées.



Le Fact Checking ou comment débusquer les Fake News :

Le terme anglais **fact-checking** se traduit littéralement comme étant l'action de **vérification des faits**. Pour aller débusquer les fake news véhiculées sur le Net, il existe plusieurs sites, gérés par des journalistes :

Hoaxbuster, le plus ancien

Depuis des années, la plateforme collaborative traque les bobards et autres rumeurs qui circulent en ligne.

Decodex, source fiable ou non ?

Le Decodex est un service en ligne proposé par le journal *Le Monde*. Il permet en entrant simplement l'url d'un site (son adresse) de vérifier sa fiabilité en matière d'informations.

Factuel, une équipe mondiale

Le blog de l'Agence France-Presse vise lui aussi à lutter contre les fausses informations propagées en ligne. Un service d'enquêtes qui traque le mensonge dans tous les domaines. Les infos sont disponibles en quatre langues.

Vrai ou fake, le fact-checking du service public

Vrai ou Fake est la plateforme de vérification de fake news de l'audiovisuel public regroupant Arte, l'Institut national de l'audiovisuel, France Médias Monde, France Télévisions, Radio France et TV5 MONDE.

Et pour les images et vidéos ?

Il est souvent possible d'identifier une fausse image ou vidéo simplement en l'observant, ou en s'intéressant au contexte dans lequel elle a été publiée. Il existe néanmoins plusieurs sites vous permettant de vérifier l'origine et le contexte de celles-ci, en voici quelques uns :

TinEye : Créé à la base pour aider les photographes à débusquer les images volées, cet outil sert également à remonter le fil de photos utilisées hors contexte à des fins d'intox, jusqu'à leur source.

Google Image : Par l'adresse de l'image (son url) ou un simple copier/coller dans la barre de recherche, Google analyse alors l'image, et va rechercher des images similaires ou sur le même thème.

CitizenEvidence : monté par Amnesty International, ce site fonctionne de la même manière, mais pour les vidéos uploadées sur YouTube.