Être connecté en toute sécurité

Pour un usage averti du numérique par les jeunes publics

Document élaboré par le groupe de travail
« Régulation et médias numériques »

الهيئة العليا للاتصال السمعي البصري
ⵓⵅⵓⵍ ⵓⵛⵜⵜⵓⵔ ⵏ ⵜⵛⵔⵓⵜⵉⵜ ⵓⵎⵣⵡⵉⵔⵣ
Haute Autorité de la Communication Audiovisuelle

"Il y a urgence à mettre en place un devoir de vigilance numérique. Enfants, jeunes et parents doivent être outillés pour naviguer dans cet océan sans fin et non sans dangers"

Groupe de travail
« Régulation et médias numériques »

Sommaire

Abréviations

ANRT: Agence Nationale de Réglementation des Télécommunications

CNDP: Commission nationale de contrôle de la protection des données à caractère personnel

HACA: Haute autorité de la communication audiovisuelle

RGPD: Règlement général sur la protection des données

HCP: Haut-commissariat au plan

DGSN: Direction générale de la sûreté nationale

ONCF: Office national des chemins de fer

UNICEF: United Nations children's fund (Fonds des Nations Unies pour l'enfance)

OMS: Organisation mondiale de la santé

FAI: Fournisseurs d'accès à internet

TIC: Technologies de l'information et de la communication

ONG: Organisation non gouvernementale

IP: Internet Protocol

URL: Uniform resource locator (Localisateur uniforme de ressource)

VPN: Virtual private network (Réseau virtuel privé)

PC: Personal computer (Ordinateur personnel)

CPS: Child Protection System (Système de protection de l'enfant)

PUBG: Player unknown's battlegrounds (Jeu vidéo multi-joueurs)

Glossaire

Deep fake : C'est une technique se basant sur l'intelligence artificielle pour permettre de créer ou modifier un enregistrement vidéo ou audio. Le mot « deepfake » est une abréviation de «Deep Learning» et «Fake», et peut être traduit par «fausse profondeur». Il fait référence à des contenus faux mais qui paraissent profondément crédibles grâce à l'intelligence artificielle.

Fact- checking : Il s'agit d'une pratique qui repose sur l'investigation pour vérifier la véracité de faits ou d'informations. Elle vise à identifier les sources d'information et dévoiler les infox qui circulent dans la sphère médiatique et numérique.

PUBG (PlayerUnknown's Battlegrounds) : Un jeu multijoueur qui consiste à trouver des armes et des ressources afin d'être le dernier survivant et remporter la partie contre une centaine de joueurs. Bien que ce jeu addictif connaisse un succès notable au niveau international, il demeure extrêmement dangereux pour la santé mentale et physique des jeunes enfants.

Pédopornographie : Il s'agit de l'exploitation des enfants et des mineurs pour la production de contenus pornographiques.

Cyberharcèlement : Le cyberharcèlement est un phénomène qui consiste à utiliser internet pour intimider, harceler, menacer ou embarrasser une personne de façon récurrente sur internet.

Pédo-criminalité : La pédo-criminalité est un délit à caractère sexuel à l'égard des enfants. Elle regroupe les abus sexuels et la pédopornographie.

Contrôle parental : Système de surveillance et de restriction pouvant être mis en place par des parents pour contrôler l'utilisation des appareils connectés (smartphones, tablettes, ordinateurs) par leurs enfants.

Cookies : Les cookies sont de petits fichiers informatiques insérés dans un ordinateur lorsqu'un site web donné est consulté. Ces fichiers conservent vos données personnelles telles que votre pseudo, votre âge, et certaines de vos habitudes de navigation, etc. Ces données sont ensuite collectées et analysées afin de faciliter votre navigation ou vous proposer des publicités susceptibles de vous intéresser.

Publicité ciblée : Technique publicitaire qui vise à identifier les personnes pendant leur navigation sur internet et collecter leurs données personnelles afin de leur diffuser des messages publicitaires spécifiques en fonction de caractéristiques individuelles.

Reciblage/retargeting : Le reciblage publicitaire est une technique de marketing en ligne permettant d'identifier les visiteurs d'un site ou d'une page web qui ont montré de l'intérêt pour un produit ou un service donnés et d'utiliser les cookies pour leur placer ultérieurement des publicités ciblées lors de leur navigation, afin d'attirer leur attention et les rediriger vers ce site en question.

Métadonnée : Il s'agit d'un type de donnée informatique caractérisant et structurant les ressources numériques contenues dans une page web.

VPN (Virtual Private Network)/Réseau privé virtuel : C'est un type de réseau informatique qui permet la création de liens directs et sécurisés entre des ordinateurs distants.

Règlement Général sur la Protection des Données (RGPD) : Entré en vigueur le 25 mai 2018, le Règlement général sur la protection des données représente le nouveau cadre européen concernant le traitement et la circulation des données à caractère personnel, ces éléments sur lesquels les entreprises s'appuient pour proposer des services et des produits.

Introduction

C'est sous l'angle du numérique qu'il faut aujourd'hui aborder la culture. La culture de l'information, et plus largement encore celle audiovisuelle, est résolument connectée. Aujourd'hui, il est pertinent de parler de cultures numériques. Des cultures plurielles dans l'univers numérique.

La Toile est devenue un fait social qui bouleverse notre manière de consommer de l'information, de l'image, du son.

Force est de constater que le numérique est l'un des principaux vecteurs de la transformation culturelle en cours. Les techniques numériques dans un monde virtuel sans frontières (et longtemps sans barrières) ont littéralement changé le rapport au monde, à l'autre et aux « choses lues, vues, entendues.»
Les jeunes publics, dont la protection est au centre des préoccupations du Régulateur, sont particulièrement exposés à ces cultures numériques de plus en plus innovantes par leurs codes et leurs normes, et qui sont véhiculées et transmises par les plateformes digitales et les réseaux sociaux.

Les parents ne sont pas forcément au courant de tout ce qui se passe lorsque leurs enfants sont seuls face aux écrans. Même s'ils le sont, ils ne réalisent pas toujours ce que cela peut représenter. Des jeunes créent des chaînes à leur nom, s'abonnent à leurs comptes préférés, postent des contenus où ils se mettent en scène, remercient leurs abonnés, les encouragent à laisser des commentaires, échangent avec des inconnus venant des quatre coins du monde. Incontestablement le Net leur offre une opportunité de s'exprimer en toute liberté et de s'affranchir de la tutelle des adultes.

Il y a urgence à mettre en place un devoir de vigilance numérique. Enfants, jeunes et parents doivent être outillés pour naviguer dans cet océan sans fin et non sans dangers. « Être connecté en toute sécurité », tel est l'objectif de ce guide qui a été élaboré dans le cadre du groupe de travail dédié à la régulation et aux médias numériques. Des outils sont proposés pour tout à la fois développer le réflexe de vérification de l'information, déceler un contenu inapproprié, protéger ses données personnelles, ou encore ne pas être exposé à l'addiction numérique.

Comment voyage un contenu partagé sur un réseau social ? Qu'est-ce qu'une infox ? Une deep fake est-elle une manipulation d'image ? Les challenges qui se multiplient sur le Net peuvent-ils représenter un danger pour les adolescents ? Ce guide apporte des réponses, propose des outils de vigilance, présente des pistes pour une navigation (presque) sans risques aussi bien pour les enfants que les parents. A l'aide d'illustrations, l'ouvrage explique également pourquoi le dialogue en toute confiance entre enfants et parents, l'exemplarité des adultes, l'instauration d'espaces sanctuarisés sans écrans à la maison ont toute leur importance.

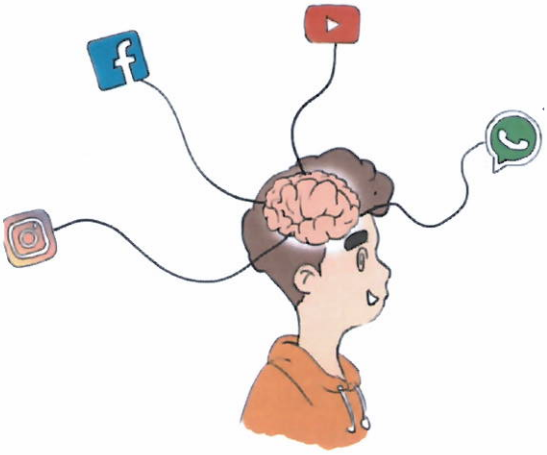
Nous vous en souhaitons bonne lecture pour une connexion en toute sécurité.

Narjis Rerhaye
Membre du CSCA
Présidente du groupe de travail « Régulation et médias numériques »

Chapitre 1

Hyper-connectivité et addiction au numérique

- Être connecté, c'est être en lien. L'accès aux technologies est un facteur de développement à plusieurs niveaux.
- Il permet de réduire les inégalités face à l'accès au savoir et à l'information.
- Le propos ne consiste donc pas à diaboliser les connectivités des plus jeunes mais à avertir sur les conséquences que peut entrainer l'excès de connectivité.
- Être connecté ! la connotation est positive.



Des expositions aux écrans de plus en plus longues

Au Maroc, selon l'enquête TIC (Technologies de l'Information et de la Communication) réalisée par l'ANRT en 2020 :

89,7% des enfants âgés entre 5 et 14 ans sont équipés d'un téléphone mobile et 85,5% d'un smartphone.

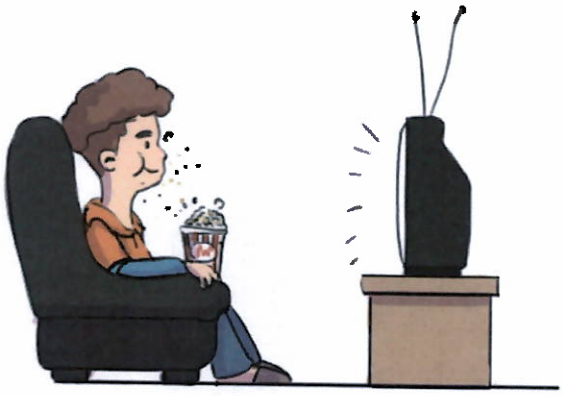
80,5% de cette tranche d'âge a accès à Internet et 75,6% d'entre eux se connectent au moins une fois par jour.

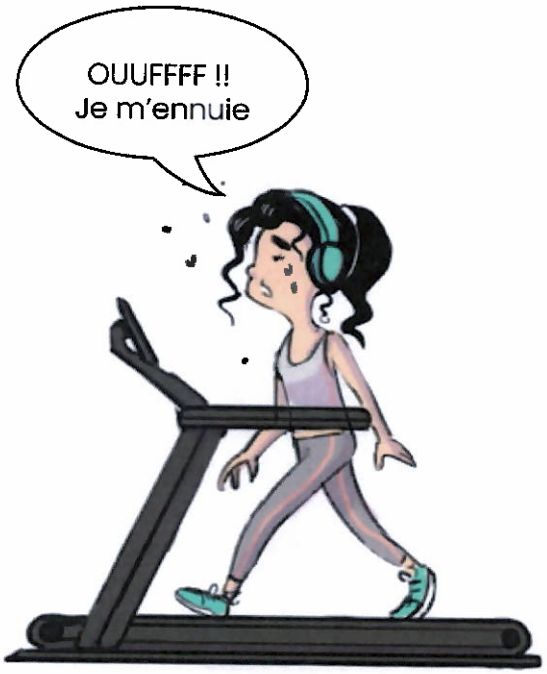
97,9% se connectent à des réseaux sociaux.

*Enquête ANRT, equipement et usages TIC en 2019.
Lien : https://www.anrt.ma/sites/default/files/publications/enquete-tic-_2019-fr.pdf

L'enquête du Haut-Commissariat au Plan sur les indicateurs sociaux (2018) fait ressortir que :

Pour les enfants de moins de 15 ans, la télévision occupe 43,6% de leur temps libre, soit une moyenne de 3h00 par jour.





Les enfants marocains ne consacrent à la pratique du sport que 2 mn et à la lecture qu'une minute par jour.

Il faut également savoir que les enfants passent 12 mn sur Internet, dépassant de 4 mn la moyenne chez les adultes (8mn) Sont enregistrées 21 mn en milieu urbain et 2 mn en milieu rural.

Les enfants utilisent Internet pour se connecter essentiellement aux réseaux sociaux. La part de cet accès allouée à des recherches éducatives ne représente que 5%.

*Les indicateurs sociaux du Maroc, édition 2020, Haut-Commissariat au Plan

L'attrait pour les écrans dès le premier âge chez les tout- petits

Les tout-petits développent une attractivité naturelle pour les écrans et deviennent quasiment anesthésiés lorsqu'on leur en met un entre les mains. Les écrans deviennent ainsi la solution à tout : pour l'occuper, pour le calmer, pour le surveiller. Résultat, de nombreux enfants en très bas âge grandissent entre biberons et écrans.

Des premiers travaux ont étudié les conséquences neuro-psychologiques de l'usage des écrans chez les tout- petits.
L'exposition des très jeunes enfants aux écrans agit négativement sur le développement du cerveau et l'apprentissage de compétences fondamentales. Les enfants surexposés aux écrans ont plus de risques de souffrir d'un retard de langage que les autres.

Comment détecter l'addiction numérique chez l'enfant ?

Quelques signaux permettent de détecter la possible installation d'une addiction

1 L'enfant n'arrive pas à contrôler le temps passé devant l'écran et en revendique davantage;

2 Il est dans le déni ou minimise lorsque la remarque lui est faite;

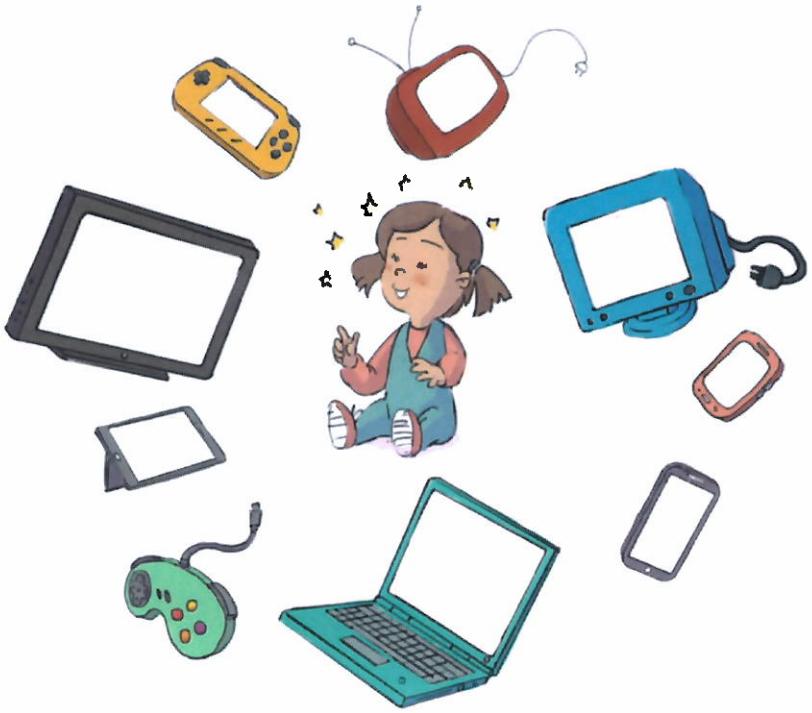
3 Le fait de ne pas pouvoir se connecter le rend agressif;

4 L'enfant se sent vide ou déprimé loin des écrans et ne manifeste pas d'intérêt pour les autres activités, même celles qu'il appréciait avant;

5 Il est plus agité, plus fatigué, moins curieux, moins concentré, ses résultats scolaires sont en baisse;

6 L'enfant se replie sur lui. Il préfère désormais les échanges en ligne aux échanges réels;

Enfants et écrans, tous responsables

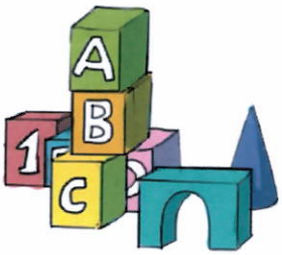


A l'âge où l'enfant développe ses capacités et aiguise ses cinq sens, l'exposition passive aux images diffusées à travers les écrans le cantonne au statut de spectateur. Ce qui «peut» dans certains «cas» altérer son développement et impacter des fonctions cognitives tel que la mémorisation, l'attention et la coordination.

L'usage des écrans à un âge précoce pour les enfants aurait des effets néfastes sur leur santé. Sommeil perturbé, prise de poids favorisée par l'inactivité ou encore troubles de la vision sont autant de dommages causés par l'exposition aux écrans sur la santé de nos enfants.

A adopter sans modération : Des recommandations émises par l'Organisation mondiale de la santé sur l'utilisation des écrans pour les enfants:

Pas d'écrans pour les enfants moins de deux ans. La lecture d'histoires et les activités physiques sont fortement recommandées.



Pas plus d'une heure devant les écrans (télévision ou jeux sur écrans) pour les enfants de plus de 2 ans. La lecture d'histoires et les exercices physiques sont conseillés.

Bien qu'il existe sur le marché plusieurs versions de tablettes éducatives ou encore de jeux éducatifs sur écrans, leur utilisation se doit d'être occasionnelle et en complément aux jeux classiques (puzzle, cubes, constructions).

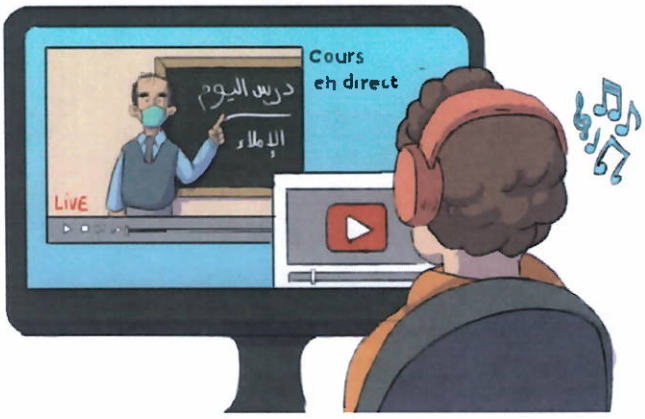
Le contrôle parental du temps d'utilisation et de la nature et les durées de connexion des enfants demeurent une obligation pour une utilisation saine et sans danger.

L'accoutumance exacerbée avec l'école à distance

L'école à distance a développé un nouveau rapport à la connexion.

De nouvelles règles ont été édictées par l'état d'ugence sanitaire imposé par la lutte contre le coronavirus. Pour apprendre et inculquer le savoir, il fallait être connecté. Ordinateurs, téléphones, tablettes ont remplacé le tableau noir.

A la maison, enfants et adolescents sont connectés à longueur de journée parce qu'ils suivent l'école en distanciel.
Naviguer seul(e) en temps de corona est-il cependant sans risques ?



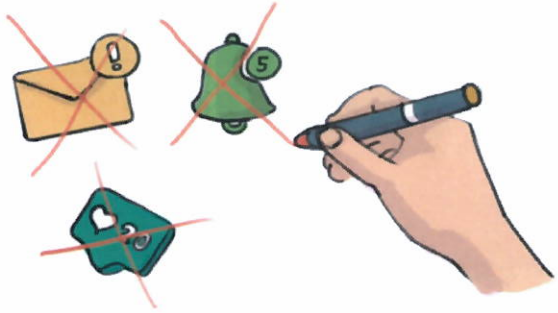
Boîte à outils

Quelles solutions pour une connexion idoine qui ne se transforme pas en addiction ?

Pour réduire l'addiction, de nombreuses techniques très simples existent :

1 L'exemplarité des parents

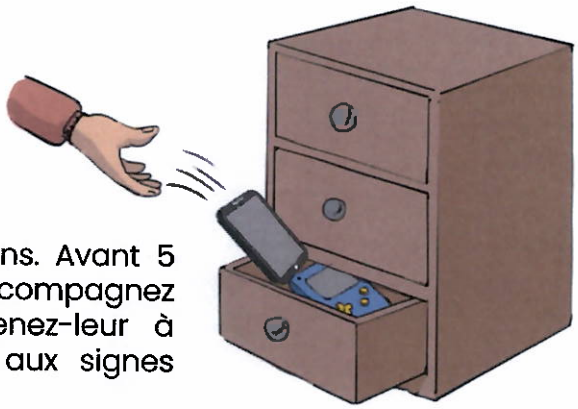
Les parents se plaignent de l'addiction de leurs enfants mais restent eux-mêmes très souvent les yeux rivés sur leurs écrans.
La préconisation première pour accompagner les jeunes publics consiste à d'abord s'appliquer à soi-même la limitation du temps d'écran.



2 La désactivation des notifications

La désactivation des notifications des applications du téléphone, pour limiter les sollicitations intempestives. Sur l'écran, on peut choisir de voir apparaitre les notifications Whatsapp, Facebook, Tik Tok et tout autre réseau social. Cela réduit les tentations de consulter son téléphone.

3 L'instauration de zones sanctuarisées sans écrans dans la maison



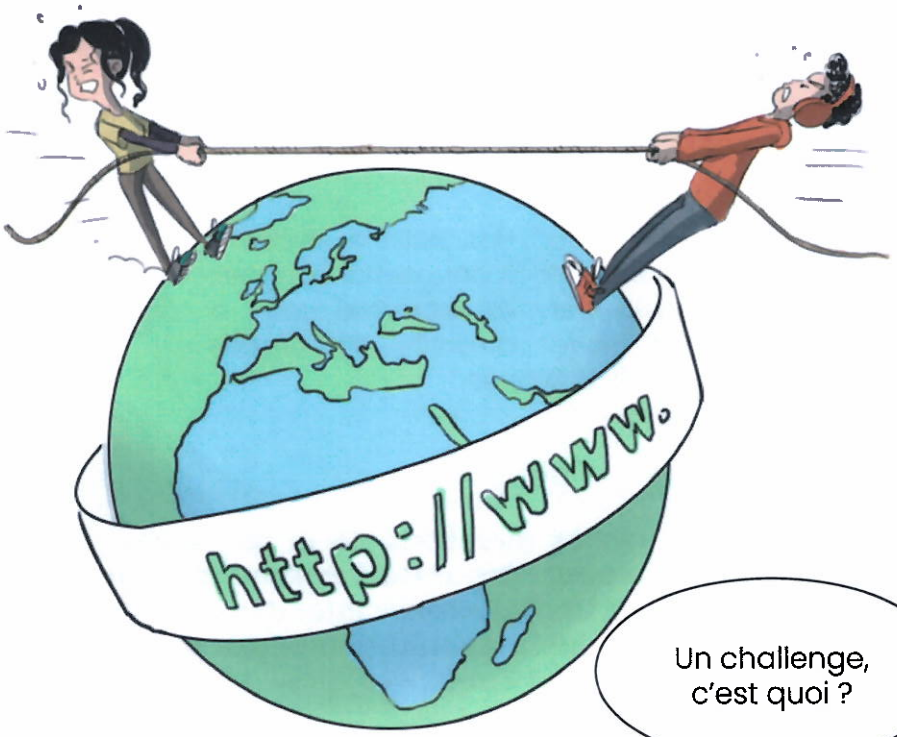
Le fait d'instaurer des espaces sans écran, permet de réduire le temps passé devant les écrans mais aussi d'installer de nouvelles habitudes.

Avant 2 ans, bannissez radicalement les écrans. Avant 5 ans, limitez les le plus possible. Avant 10 ans, accompagnez vos enfants dans leur navigation et apprenez-leur à s'auto-réguler. Après 10 ans, soyez attentifs aux signes d'accoutumance et aux résultats scolaires.

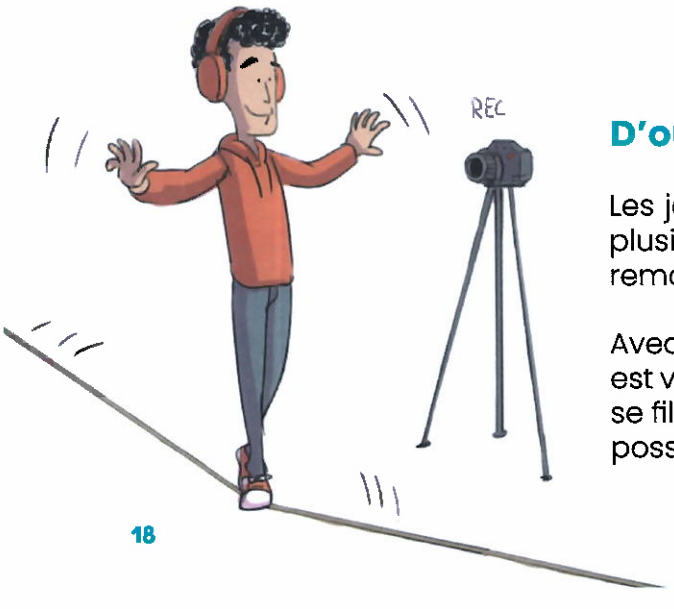
Selon les nouvelles directives de la santé des jeunes enfants publiées par l'Organisation Mondiale de la Santé en 2019, l'âge de bannissement total des écrans est fixé à deux ans. Certains préconisent même d'éradiquer les écrans avant l'âge de 3 ans.

Chapitre 2

Les défis sur Internet ciblant le jeune public



Ils sont de plus en plus nombreux sur la Toile. Les challenges ou défis ont investi le Net , allant du simple jeu entre amis au drame mortel.
Les challenges vont du défi inoffensif, souvent drôle, à celui dangereux qui conduit à toutes les dérives, voire à la mort.
Un défi se fait généralement entre amis et se partage sur les réseaux sociaux. Ce qui explique sa forte dimension virale.
De nouveaux défis naissent régulièrement sur Internet. Leur succès auprès des jeunes est variable. La vigilance est de rigueur car généralement, l'implication dans ces défis de jeunes se fait à l'abri des regards et dans le secret d'une chambre d'ado.



D'où viennent ces jeux de défi?

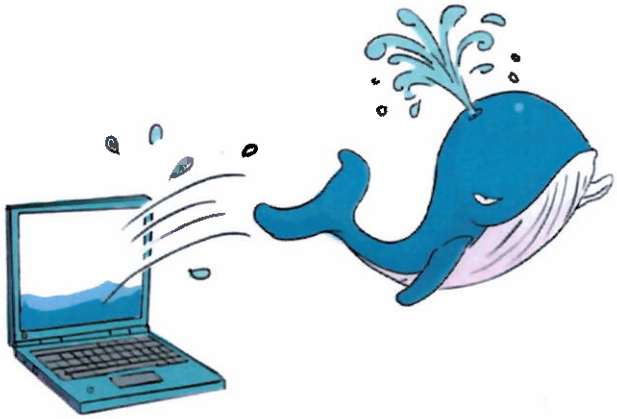
Les jeux de défis et les jeux dangereux existent depuis plusieurs décennies. Les premiers challenges recensés remontent aux années 1950.

Avec Internet et les réseaux sociaux, leur caractère viral est vite devenu inévitable. En se prenant en photo ou en se filmant, les participants à ces challenges s'offrent la possibilité d'une diffusion planétaire et sans frontières.

Challenges sur les réseaux : les risques pour la santé

Pour être vigilant, il faut être informé et en savoir le plus possible sur ces défis numériques qui peuvent conduire à l'irréparable.

Voici une liste noire et non exhaustive des challenges en ligne les plus dangereux. Beaucoup d'entre eux n'ont pas été un phénomène viral sur la Toile marocaine. D'autres ont eu leurs amateurs au Maroc.



Le défi de la Baleine bleue

Apparu en Russie en 2015, le blue whale challenge ou défi de la Baleine bleue a été médiatisé après le suicide d'une jeune fille. Dans la plupart des pays d'Europe, le Blue Whale Challenge a surgi au printemps 2017, lorsque la presse s'est fait l'écho de nombreux suicides de jeunes adolescents en Russie, à la suite de ces mystérieux défis qui se sont manifestés sur Internet. Le concept du Blue Whale Challenge reposerait sur l'existence d'énigmatiques tuteurs qui, par le biais de réseaux de discussions secrets, entreraient en contact avec de nombreux jeunes en leur demandant de relever cinquante défis. Ces défis, très simples et bon enfant au début, connaîtraient par la suite une montée en puissance dont l'étape ultime serait le suicide.

Le Fire challenge

Le "Fire Challenge" pour lequel les adolescents s'enduisent une partie du corps (torse, jambe, bras...) d'alcool, d'allume-feu ou de tout liquide hautement inflammable, et allument le briquet... Les plus prudents pratiquent le Fire Challenge sous la douche. L'objectif étant d'éteindre les flammes le plus rapidement possible. Malheureusement, les joueurs sont souvent très vite dépassés par les évènements, et certains tellement saisis par la douleur qu'ils en perdent leurs moyens et ne sont plus capables d'ouvrir l'eau pour etteindre le feu qui les brûle.

Skull breaker challenge

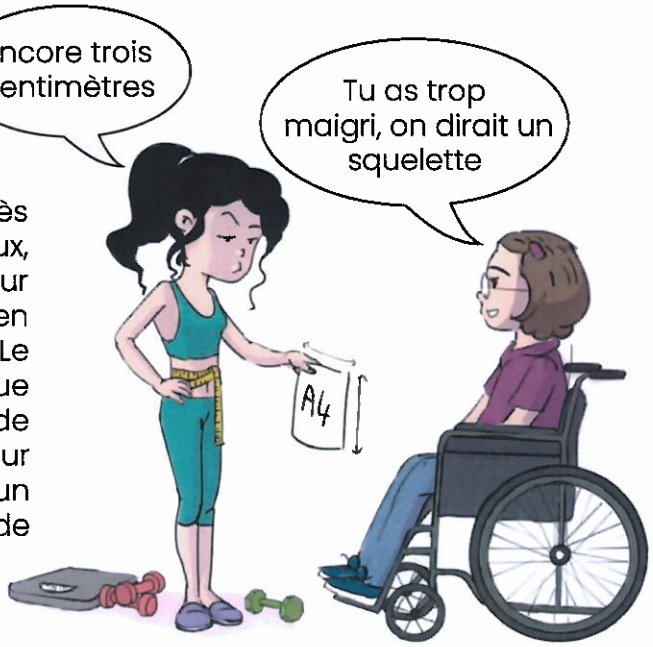
Le principe de ce jeu, apparu initialement au Venezuela, consiste à ce que trois personnes se tiennent sur la même ligne. La personne au milieu, ne devant pas être au courant du challenge, saute lorsque les deux autres saisissent l'occasion pour lui donner un coup de pieds derrière le tibia, provoquant une chute dangereuse sur le dos. Le challenge est également pratiqué par les adultes, entraînant des pertes conscience , des commotions cérébrales ou des paralysies.

Le jeu du foulard

Le jeu du foulard est le cauchemar des parents et des enseignants. Il s'agit d'un étranglement volontaire, souvent réalisé par un groupe de jeunes pour connaître des sensations nouvelles. Une expérience extrême qui peut provoquer des séquelles irréversibles ou la mort.

A4 Challenge

Le A4 challenge est un défi né en Chine. Très suivi par les filles sur les réseaux sociaux, il est particulièrement dangereux pour la santé. Il s'agit de se photographier en plaçant une feuille A4 devant son ventre. Le challenge réside dans le fait de montrer que le ventre ne dépasse pas de la feuille et de prouver que la fille en question a la minceur d'une top model. En plus de véhiculer un message négatif, il a exposé à l'anorexie de nombreuses internautes.



Le Momo challenge

Harcèlement, menaces, piratage, incitation au suicide... le Momo Challenge a longtemps encouragé les joueurs à commettre des actes dangereux en les menaçant. C'est sur la messagerie Whatsapp que le Momo Challenge s'est fait connaître, a pris possession du web et plus particulièrement de WhatsApp. C'est via la messagerie que les internautes peuvent contacter un numéro inconnu, partagé sur Reddit ou Facebook.

Boîte à outils

La prévention, une règle en or

Prévenir passe ici par informer, dialoguer, discuter avec ces jeunes amateurs, ou pas, de défis sur la Toile.
Les challenges mêlent à la fois jeu et violence. Il faut expliquer la prise de risque dans de tels défis. Il y a des défis dangereux qui peuvent conduire à la mort. Il faut savoir l'expliquer aux adolescents.

Il est également important de déconstruire la perception d'appartenir à un groupe. Les jeunes qui participent à un défi lancé sur le Net sont dans une sorte de quête d'appartenance au groupe. C'est dans ce sens que la surenchère est de mise : aller toujours plus loin, ne pas reculer, et surtout, relever à n'importe quel prix le challenge.

1 Informer sur les dangers d'un challenge est une démarche essentielle;

2 S'informer aussi pour rester en alerte par rapport aux derniers défis numériques;

3 Suivre par l'historique des moteurs de recherches consultés par l'ado;

4 L'enfant doit savoir qu'il ne sera pas interdit d'Internet ou des réseaux sociaux s'il porte un intérêt à un défi. La crainte de la confiscation ou de la sanction ne doit pas devenir un obstacle au dialogue.

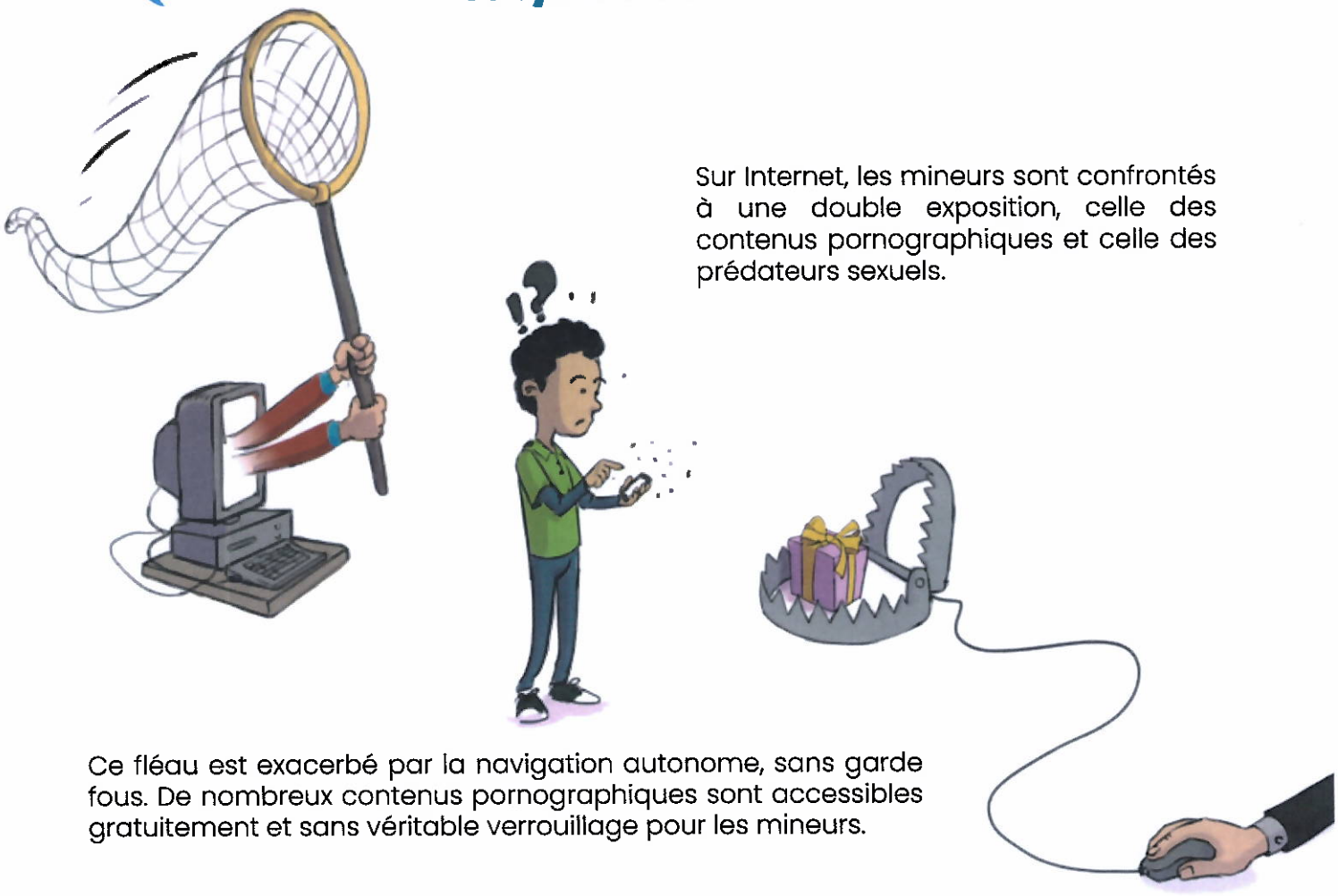
Un challenge sur Internet ou sur les réseaux sociaux peut être positif.

Il en existe des centaines, tous les jours.

Remercier 5 personnes dans la journée, se rendre utile pour un proche, dire à sa mère et à son père qu'on les aime.

Chapitre 3

Pédocriminalité, pédopornographie et cyberharcèlement

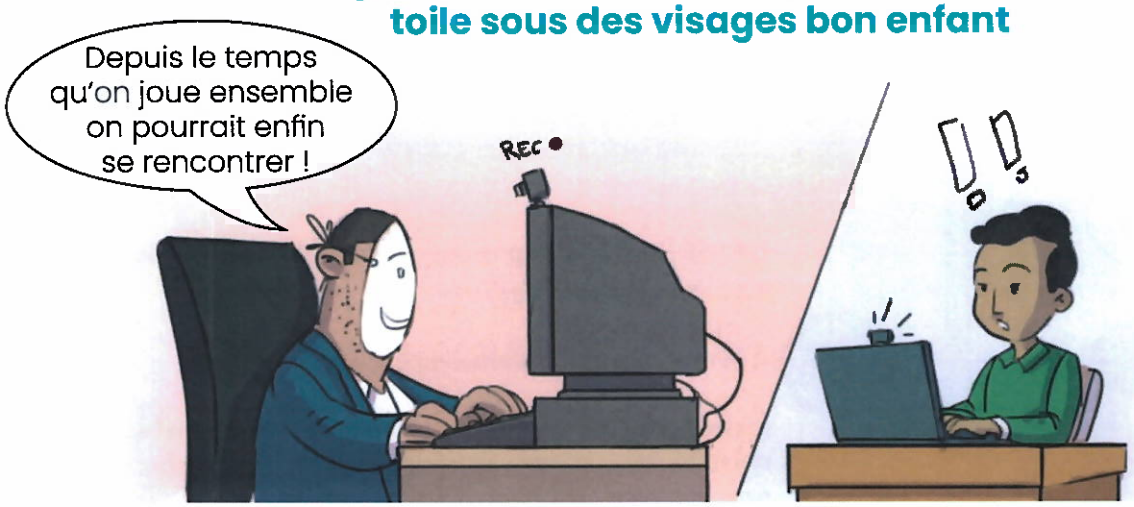


Sur Internet, les mineurs sont confrontés à une double exposition, celle des contenus pornographiques et celle des prédateurs sexuels.

Ce fléau est exacerbé par la navigation autonome, sans garde fous. De nombreux contenus pornographiques sont accessibles gratuitement et sans véritable verrouillage pour les mineurs.

En 2009, selon les chiffres de l'Organisation des Nations Unies, plus de 750 000 prédateurs sexuels auraient été connectés sur le réseau. Des estimations indiquent qu'un enfant sur cinq reçoit des sollicitations sexuelles sur la Toile.

Les prédateurs se cachent parmi nous sur la toile sous des visages bon enfant



Attention ! L'exposition précoce à la pornographie peut être lourde de conséquences en matière de santé mentale. Elle peut notamment générer des troubles de la sexualité.

Il n'existe pas de profil type de cyber pédo-criminels.

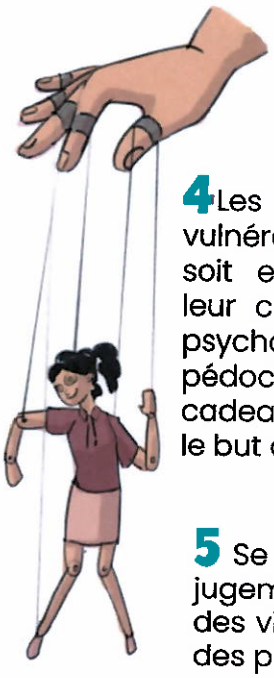
On peut toutefois distinguer deux catégories de cyber pédo-criminels :
-Des amateurs de pornographie juvénile (dits cyber-voyeurs)
-Des agresseurs sexuels d'enfants qui utilisent Internet communément appelés cyber -prédateurs

Les cyber pédo-criminels infiltrent les groupes au sein des réseaux sociaux Facebook, Instagram et Snapchat mais aussi les jeux en ligne. Ils piratent des photos de profil de jeunes utilisateurs, se font passer pour eux, et installent une confiance avec leur victime afin de mieux les approcher.

Une étude menée en 2019 par l'ONG Action Innocence basée en Suisse révèle que :

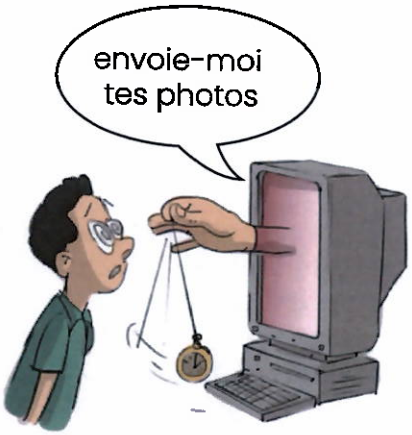
1 Les victimes sont souvent abordées sur des tchats et forums réservés aux mineurs. Les pseudos ou les informations (âge, sexe, localisation géographique) qu'ils ont mises dans leur profil sont les principaux éléments qui déclenchent l'attention des cyber pédo-criminels.

2 Les échanges se font ensuite via les messageries personnelles et par téléphone à fréquence régulière.



3 Une relation de confiance s'établit au fur et à mesure des discussions.

4 Les cyber pédo-criminels exploitent la vulnérabilité émotionnelle des adolescents, soit en répondant à des questions liées à leur curiosité sexuelle, soit en les manipulant psychologiquement. Dans certains cas , les pédocriminels n'hésitent pas à tenter d'offrir des cadeaux ou des récompenses aux victimes dans le but de les séduire.



5 Se basant sur la confiance avec des jeunes qui manquent encore de jugement et d'expérience, les pédocriminels en ligne peuvent réclamer des vidéos et images intimes ou encore une rencontre physique à l'insu des parents.

Le cyber-harcèlement : Les femmes en première ligne

L'accès aux technologies de l'information et de la communication se fait en un clic

Smartphones, tablettes, PC et autres objets connectés sont à portée de main. Et avec le développement des réseaux sociaux, le phénomène du cyber- harcèlement prend une ampleur inédite auprès des plus jeunes.

Plusieurs formes d'agressions en ligne sont assimilées au cyber-harcèlement : propagation de rumeurs et dénigrement, usurpation et piratage de données personnelles, insultes, moqueries et intimidations en ligne, extorsion, ou encore chantage sexuel.

.

Les conséquences de ce phénomène se répercutent directement sur la santé mentale et le bien-être des victimes et peuvent présenter des dommages irréversibles tels que le suicide, la dépression et la perte d'estime de soi.

Les femmes, deux fois plus harcelées en ligne que les hommes

Au Maroc, et selon le rapport annuel de l'Association Tahadi pour l'égalité et la citoyenneté publié au titre de 2020, les femmes victimes de cyberharcèlement sont majoritairement des collégiennes, lycéennes et étudiantes.
Le harcèlement est l'acte de violence numérique le plus répandu.
Menaces, diffamation, envoi de messages à caractère sexuel, chantage sexuel font partie de ces violences numériques répertoriées par ce rapport.
WhatsApp est le premier réseau social où surviennent ces actes. Il est suivi de Facebook, Instagram et Messenger.
Un peu partout dans le monde, les femmes sont deux fois plus harcelées en ligne que les hommes.

Au Maroc, ce que dit la loi sur le harcèlement

Article 503-2 du code pénal : «Est coupable de harcèlement sexuel et puni de l'emprisonnement d'un an à deux ans et d'une amende de 5.000 à 50.000 dirhams, quiconque, en abusant de l'autorité qui lui confère ses fonctions, harcèle autrui en usant d'ordres, de menaces, de contraintes ou de tout autre moyen, dans le but d'obtenir des faveurs de nature sexuelle».

L'arsenal juridique marocain s'est également renforcé par la loi 103-13 du 22 février 2018 relative à la lutte contre les violences faites aux femmes qui punit le harcèlement en ligne. « Est coupable de harcèlement sexuel et est qui puni d'un emprisonnement d'un mois à six mois et d'une amende de 2.000 à 10.000 dirhams ou de l'une de ces peines, quiconque persiste à harceler autrui dans les cas suivants :

1. Dans les espaces publics ou autres, par des agissements, des paroles, des gestes à caractère sexuel ou à des fins sexuelles ;
2. Par des messages écrits, téléphoniques ou électroniques, des enregistrements ou des images à caractère sexuel ou à des fins sexuelles »

Enfin, le Maroc a ratifié la convention internationale sur la cybercriminalité dite convention de Budapest, en vigueur depuis le 01/10/2018. Grâce à cette ratification, les autorités judiciaires marocaines peuvent poursuivre les cybercriminels transfrontaliers, et en particulier les cyber-harceleurs.

Boîte à outils

Comment protéger les enfants des prédateurs du Net ?

1 Le contrôle parental

Plusieurs outils numériques de contrôle parental permettent de limiter le risque d'exposition aux images pornographiques. Il est possible de télécharger, sur l'appareil des parents et des enfants, des applications ou d'installer des logiciels qui détecteront les contenus inappropriés et empêcheront l'accès aux sites pornographiques.

C'est aux parents d'activer ces applications et de les configurer afin de les protéger de la désactivation ou du paramétrage à travers un mot de passe.

Ces outils permettent également de bloquer l'accès à d'autres contenus inadaptés aux mineurs (par exemple, les contenus violents, les sites de jeux d'argent, etc.), ou encore de définir la durée maximale ou les plages horaires d'utilisation d'un appareil.

Il existe en ligne de nombreuses offres de contrôle parental, payantes ou gratuites. Le plus simple est d'utiliser les outils fournis par votre opérateur mobile ou internet, ou encore ceux intégrés dans le système d'exploitation de l'appareil de votre enfant.

Quelques outils en accès libre à la disposition des parents

Ordinateur

Contrôle parental pour Mac OS

https://www.apple.com/fr/families/

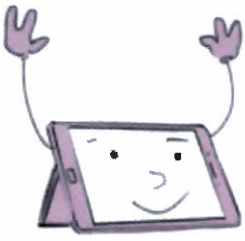
Contrôle parental pour Windows
https://account.microsoft.com/family/about

smartphone

IPhone : Temps d'écran

https://www.apple.com/fr/families/

Android : Family Link, outil de contrôle parental de Google
https://families.google.com/intl/fr/familylink/



Tablette

IPad : Temps d'écran
https://www.apple.com/fr/families/

Android : Family Link, outil de contrôle parental de Google
https://families.google.com/intl/fr/familylink/

*Ce guide propose des solutions à titre indicatif, certaines solutions peuvent être soumises à conditions

Les fournisseurs d'accès à Internet (FAI) ne fournissent pas d'application en ligne mais prodiguent des conseils.

Maroc Telecom

Maroc Telecom propose un Service (payant) de contrôle parental **Kaspersky Safekids**.

Cette application offre plusieurs fonctionnalités : gestion du temps d'écran, contrôle du temps passé sur les réseaux sociaux, blocage de contenus inappropriés, tracking de la localisation, etc

Service (gratuit) de contrôle parental "**Norton Family**".
Maroc Telecom propose gratuitement à ses clients ce service qui permet aux parents de suivre et de sécuriser l'accès à Internet de leurs enfants.

Il permet notamment la supervision et/ou le blocage de l'activité web ainsi que le déclenchement d'une notification automatique par courrier électronique lorsque les enfants ignorent un avertissement et tentent de visiter des sites web inappropriés.

Service « « **Smart Kids** » » qui permet aux parents de localiser leur enfant à tout moment grâce à une balise connectée.

INWI

Application ludo-éducative Damir de la rubrique "espaces enfants" sur le site d'Inwi. A priori, elle est toujours fonctionnelle. Toutefois, il faut être client d'Inwi pour pouvoir la tester via le magasin d'applications de son smartphone.

Partenariats avec l'UNICEF (campagnes de sensibilisation auprès des parents, des enfants et des éducateurs).

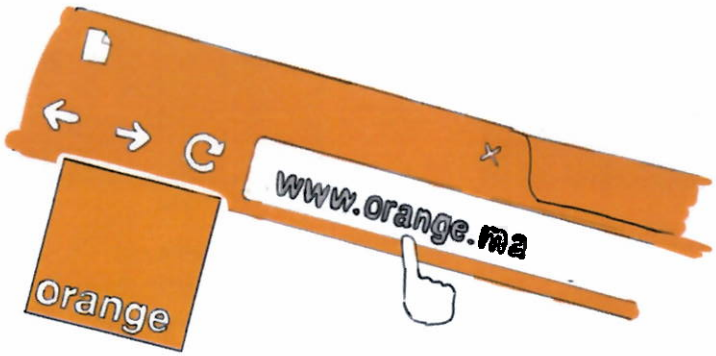
Inwi propose également des outils de contrôle parental, comme l'application "**Xooloo App Kids**".

Orange

Orange.ma a une page dédiée à la sensibilisation concernant les jeunes publics.

https://corporate.orange.ma/Bien-Vivre-Le-Digital/Usage-responsable/Usage-responsable/Votre-enfant-joue-aux-jeux-video-que-savoir

« Bien vivre le digital » propose des actions de sensibilisation au profit des écoliers et des ateliers gratuits pour initier les jeunes au codage informatique, ainsi qu'un guide des usages positifs des écrans.



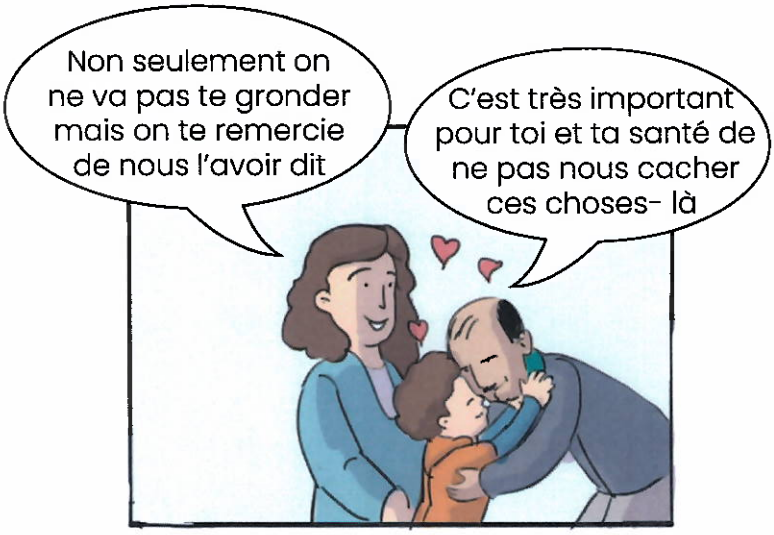
*Ce guide propose des solutions à titre indicatif, certaines solutions peuvent être soumises à conditions

2 Le dialogue

L'outil de contrôle parental réduit certes les risques d'exposition de vos enfants aux images pornographiques mais ne les prémunit pas totalement.

C'est pourquoi il est essentiel de dialoguer et de ne pas les culpabiliser s'ils ont été confrontés à des images choquantes.

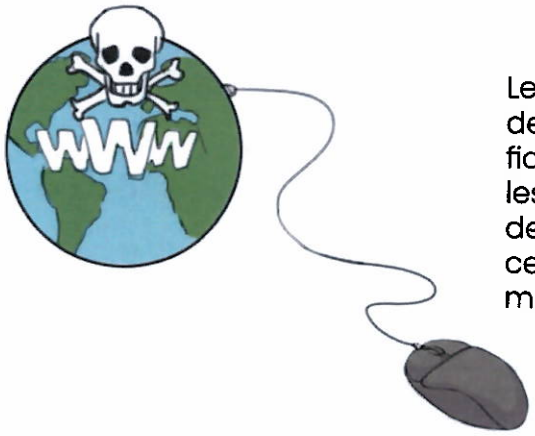
Parfois, les enfants n'osent pas parler de ce qu'ils ont vu de peur d'être grondés et/ou privés d'écrans. La dimension de la honte –« hchouma »- doit être aussi prise en considération. Encouragez les enfants à se confier.



Et pour finir

Un logiciel mondial pour lutter contre les abus d'enfants

Grâce à un logiciel baptisé Child Protection System (CPS) utilisé dans 50 États américains et dans 96 pays, 12 448 délinquants ont été arrêtés et plus de 600 000 cas de maltraitance infantile ont été évités. Toutefois, ce dernier chiffre est encore très faible par rapport aux cas déclarés.
C'est ce qui a amené l'ONG à demander une collaboration avec les plateformes de médias sociaux pour améliorer l'efficacité du dispositif. D'ailleurs, le logiciel fait face à des problèmes croissants de confidentialité, ce qui constitue un frein à son développement.
Cet outil est utilisé par 12 000 enquêteurs dans le monde entier.



Les plateformes pédopornographiques permettent de partager, de télécharger et de visualiser des fichiers gratuitement. Elles sont similaires à celles que les internautes utilisent pour télécharger illégalement des films ou des logiciels. Les personnes qui vont sur ces plateformes pensent qu'elles sont anonymes, mais ce n'est pas le cas.

CPS affiche sur une carte la localisation et l'adresse IP des ordinateurs qui ont récemment téléchargé, via les plateformes surveillées par le logiciel, des images ou des vidéos déjà signalées ou saisies par la police. La technologie dispose d'une base de données régulièrement mise à jour et contenant 18,5 milliards d'enregistrements.
L'outil va ensuite trier les cas détectés avant de se concentrer sur les délinquants les plus persistants, ceux-ci étant plus à risque.

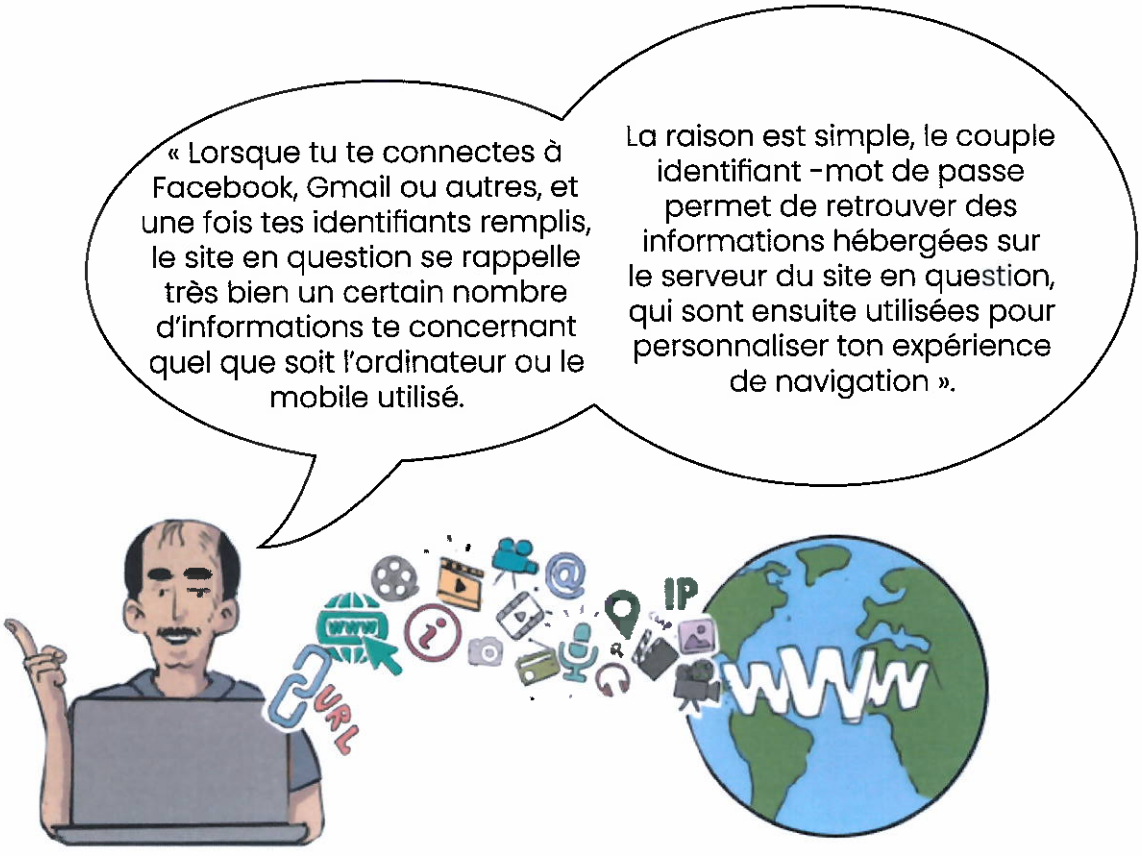
Chapitre 4

Données personnelles : comment les protéger ?

Les « données à caractère personnel » sont au centre de toutes les préoccupations.
Internet oblige, nous sommes de plus en plus amenés à partager ce type de données.
Le moindre abonnement pour suivre un site, la moindre inscription à un réseau social ou à un jeu collectif en ligne conduit à partager une quantité de données dites personnelles qui sont ensuite transmises d'une société à l'autre.
Pour éviter que nos données personnelles soient partagées, des lois ont été créées pour les protéger.

Une donnée personnelle : c'est quoi au juste ?

Un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.
Lorsque l'on visite un site pour la première fois, un certain nombre d'informations sont fréquemment demandées. Ces informations permettent de personnaliser la connexion au site en question.



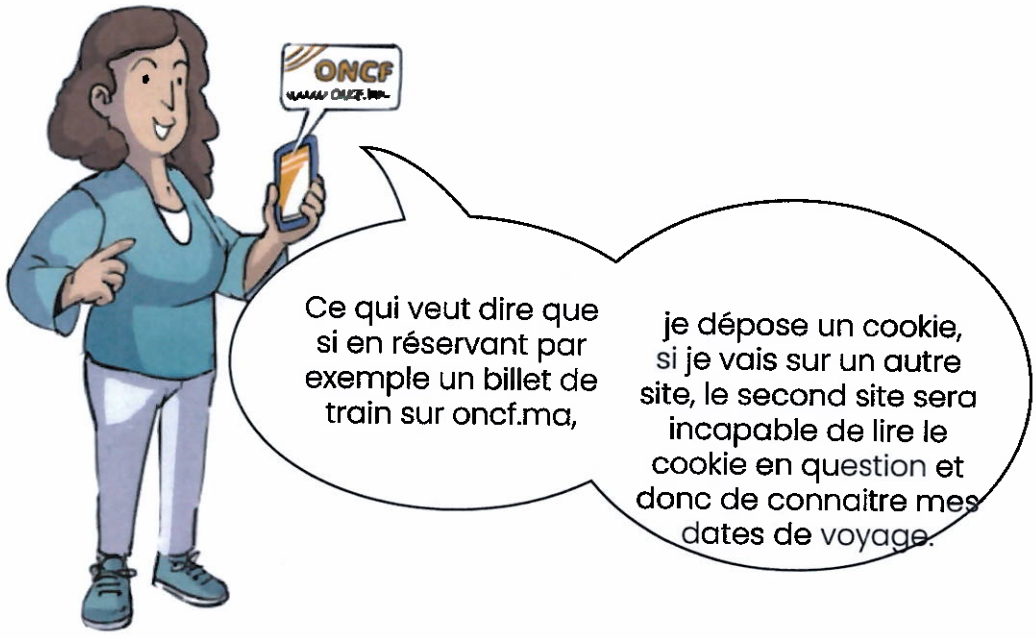
Faut-il accepter les cookies ?

Attention, selon la loi 09-08 un site Internet qui utilise des cookies faisant appel à des données personnelles doit recueillir le consentement de l'internaute avant le dépôt de ces cookies. De même qu'il doit préciser la finalité de l'utilisation des cookies et expliquer à l'internaute les moyens de s'y opposer.

Depuis les débuts du web, les cookies ne peuvent être lus que par les sites qui les ont déposés. Seul le site qui a stocké cette information pourra y accéder par la suite tant qu'elle n'est pas arrivée à péremption.

Des questions et des réponses pour mieux comprendre

Y a-t-il réellement un quelconque souci de confidentialité avec les cookies ?
Pourquoi une loi oblige-t-elle tous les éditeurs de sites web à demander explicitement l'accord de l'internaute dès sa connexion à tel ou tel site ?
Si tu surfes avec le navigateur Chrome par exemple, tu peux voir tous tes cookies et les domaines auxquels ils sont confinés en appuyant sur F12 puis Ressources > Cookies.



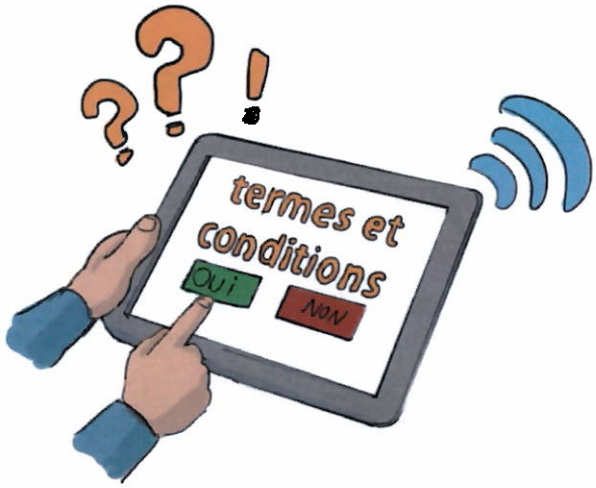
*La loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

Peut-on refuser les cookies ?

Les régies publicitaires déposent des cookies pour vous tracker : Quand vous chargez une page avec de la publicité, Google va déposer ou mettre à jour un cookie dans lequel il va stocker des informations relatives à la page consultée.

Vous recevrez ensuite des publicités ciblées en lien avec vos recherches. Ce sont des cookies qui ont pour fonction de faire du reciblage.

C'est ce principe de reciblage ou « retargeting » qui donne l'impression d'être suivi à la trace sur le web.
Source PXAgency : https://pxagency.fr/cookies-internet-accepter/?utm_source=cpp



Diktat des cookies et consentement des utilisateurs, restez informés sur vos droits

Les termes et conditions souvent longs et auxquels les utilisateurs n'accordent que peu d'importance constituent la première porte d'accès à vos données personnelles.
Ainsi, la question du consentement se pose avec acuité dès lors que la consultation du site internet est conditionnée par l'acceptation des cookies et conditions d'utilisation parfois très complexes à comprendre.

Que dit la loi au Maroc ?

Au Maroc, les lignes directrices relatives à la conformité des sites web définissent le cadre d'utilisation des cookies. « Un site internet qui utilise des cookies faisant appel à des données personnelles doit recueillir le consentement de l'internaute avant le dépôt de ces cookies. De même qu'il doit préciser la finalité de l'utilisation des cookies et expliquer à l'internaute les moyens de s'y opposer ».
Le Règlement Général sur la Protection des Données (RGPD) en vigueur depuis le 25 Mai 2018 précise que « conditionner la fourniture d'un service à une collecte de données non indispensable à celle-ci fait obstacle au recueil d'un consentement libre. Ainsi, la consultation du site ne peut pas être « bloquée » en cas de refus de dépôt de cookies ».

Pour aller plus loin, voir les publications de la Commission nationale de contrôle de la protection des données à caractère personnel.

https://www.cndp.ma/images/documents/BD-CNDP-fr.pdf
https://www.cndp.ma/images/documents/CNDP-guide-conformite-sites-web-fr.pdf

Boîte à outils

De bonnes pratiques pour une gestion optimale de vos données personnelles

La protection de la vie privée et des données personnelles est comme un combat individuel face à un monde numérique façonné par la collecte et le stockage massifs des données à des fins commerciales et marketing.
En tant qu'utilisateur, la prise de conscience de l'importance du patrimoine informationnel doit se faire dès les premiers clics.
A chaque utilisation, des traces de navigation, les cookies et encore des métadonnées sur le comportement numérique de l'internaute sont stockés et peuvent être utilisés à des fins de ciblage publicitaire.

Afin d'assurer la sécurité des données personnelles, voici quelques bonnes pratiques à adopter sans modération:

1 Désinstaller les applications et programmes superflus du smartphone et de l'ordinateur;

2 Désactiver les données de localisation et réinitialiser les permissions accordées aux services;

3 Réinitialiser l'identifiant publicitaire;

4 Utiliser le chiffrement du contenu sur smartphone et sur ordinateur;

5 Utilisez un VPN sécurisé (VPN : réseau privé virtuel, autrement dit, un logiciel qui va créer un tunnel sécurisé entre l'usager et Internet);

6 Paramétrer un pare-feu bloquant les connexions entrantes indésirables;

7 Utiliser un navigateur Internet et un moteur de recherche respectueux de la vie privée;

Il existe plusieurs outils et logiciels respectueux de la confidentialité des données personnelles.

Ce guide propose, à titre indicatif et de façon non exhaustive, quelques outils disponibles et gratuits pour mieux protéger vos données personnelles.*

Le site **Panopticlick** permet de tester la résistance du navigateur au fingerprinting — la reconnaissance du navigateur parmi la masse.

Le navigateur **Brave** permet le blocage natif des publicités et traceurs en ligne ainsi qu'un système de récompenses facultatif lié à des publicités dites convenables et qui permettent de verser un pécule à un créateur de contenu.

Keepass outil open source et gratuit permettant de stocker les mots de passe sur une base de données unique, verrouillée par une clé maîtresse ou un fichier clé.

Signal, véritable alternative à l'application whatsApp, cette solution très populaire financée par des dons utilise le chiffrement de bout en bout.

Privacy badger est une extension pour navigateur internet permettant d'empêcher les trackers publicitaires de surveiller secrètement votre activité sur le web. Si un publicitaire semble vous guetter sur les multiples pages web sans votre permission, il sera automatiquement bloqué et ne pourra plus afficher de contenu.

* Il faut toutefois noter que ces logiciels peuvent changer de mode d'accès ou devenir obsolètes.

Chapitre 5

LE FACT-CHECKING en 5 conseils

1 Identifier l'auteur du message

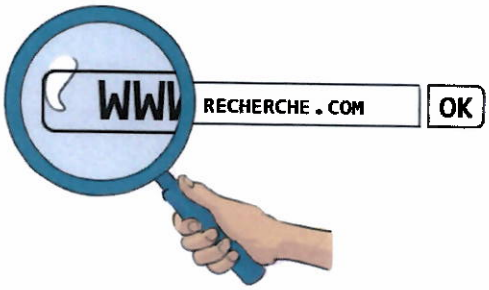
Qui s'exprime ? S'agit-il d'un média connu, d'une personnalité publique ou bien d'un site ou d'un internaute dont vous n'avez jamais entendu parler ?

En cas de doute, il faut toujours consulter des sources identifiées comme sûres et reconnues.

2 Adopter le principe qu'une information donnée sur le Web par un inconnu est par défaut plus fausse que vraie

Il est toujours plus prudent de se fier aux médias reconnus, aux journalistes et aux experts identifiés. Mais attention, cela ne suffit pas pour autant à rendre leurs informations vraies.

3 Recouper le message, une fois la source identifiée



Si plusieurs médias fiables donnent la même information en citant des sources différentes, celle-ci a de bonnes chances d'être avérée.
A l'inverse, face à une information non sourcée, le fait de ne pas en retrouver la mention ailleurs invite à la plus grande prudence.

4 Remonter à la première source dans la mesure du possible

Beaucoup de messages qui circulent sur les réseaux sociaux ne disent pas d'où provient l'information.

L'idée à retenir est qu'il vaut mieux entendre directement une conversation que de se fier au récit de quelqu'un qui a parlé à quelqu'un qui y a assisté.

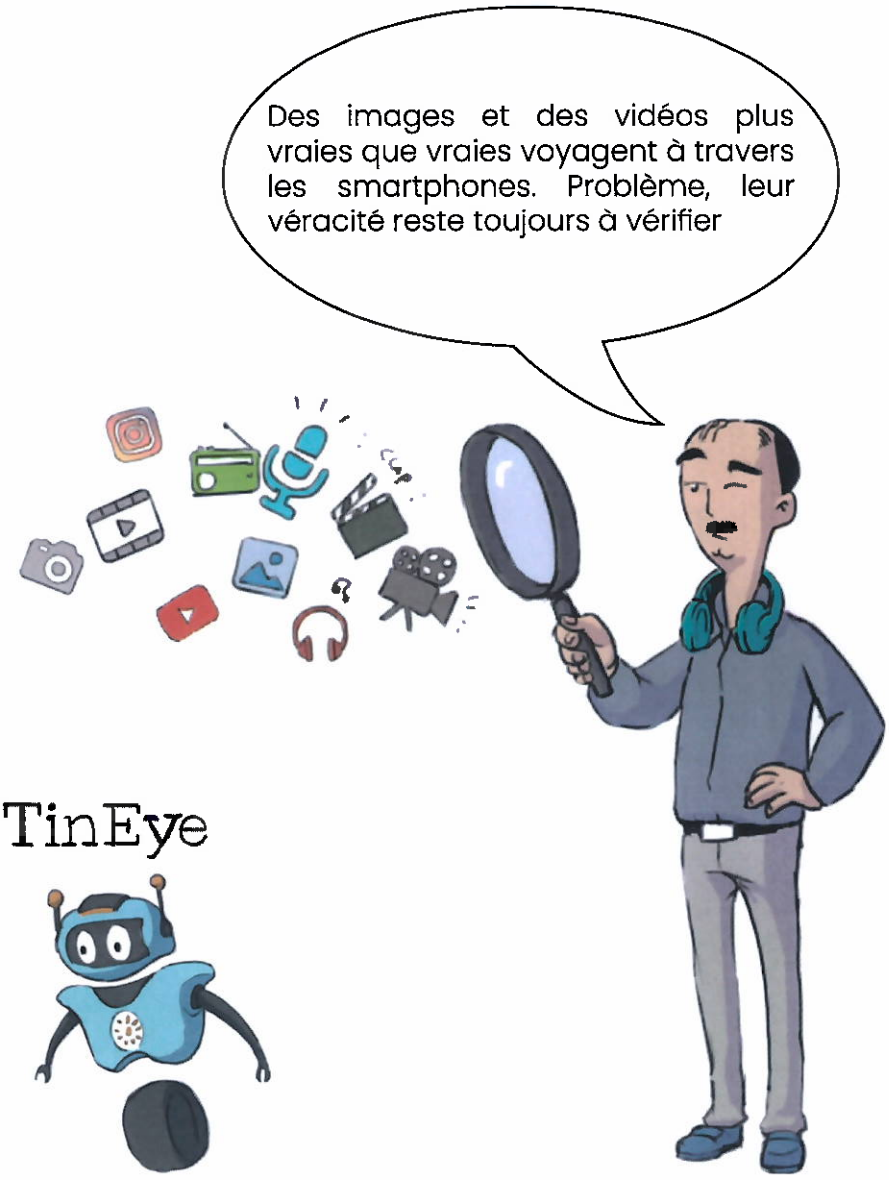
Les sources indirectes, du type « le mari d'une amie d'un collègue » ou « L'ami d'un ami » ainsi que les sources prétendument institutionnelles mais très floues comme « quelqu'un qui travaille à la police/à la DGSN /dans l'armée... » sont donc à éviter.

5 Il faut toujours se dire que plus une information est surprenante, plus elle doit être étayée et précise.

Méfiez-vous également des fausses évidences, du type « tout le monde sait que... » ou « inutile de démontrer que... »

Boîte à outils

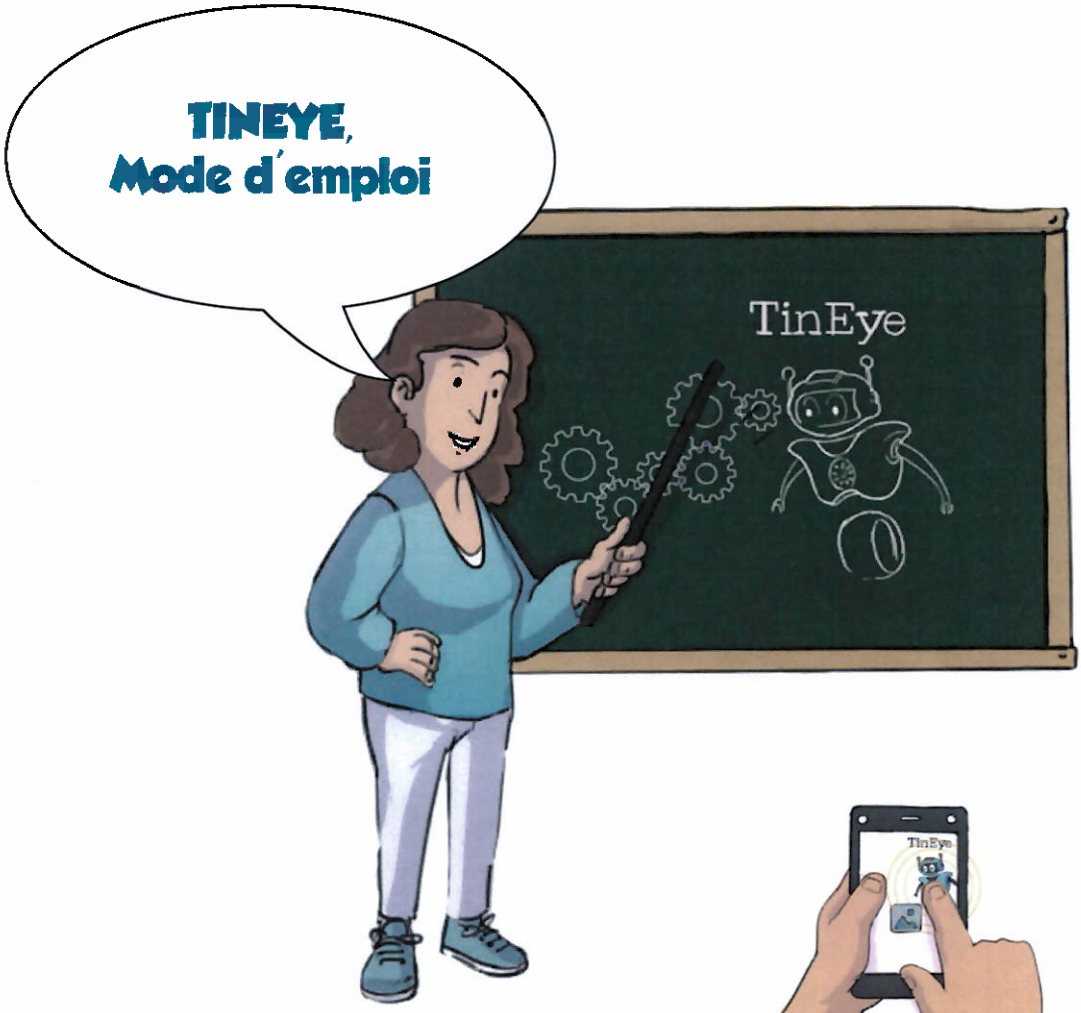
Comment faire seul(e) du FACT-CHECKING ?



Comment vérifier les images sur un smartphone :

TinEye est un outil gratuit de recherche d'images inversées sur les stéroïdes. « Reverse image search » est comme un moteur de recherche de photos. On peut donc trouver d'autres endroits en ligne où la même image, ou une image similaire, a été publiée.

TINEYE, Mode d'emploi

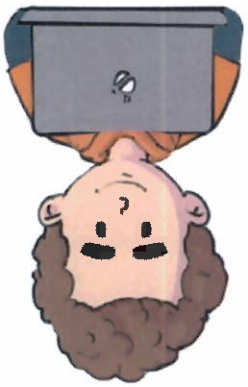


1 Il faut enregistrer ou télécharger la photo à vérifier en appuyant et maintenant l'image sur l'écran jusqu'à ce qu'apparaisse l'option pour l'enregistrer. OU Copier l'adresse Web de l'image objet de la vérification.

2 Accéder à http://www.tineye.com dans le navigateur de votre téléphone. Sélectionner « télécharger l'image » et rechercher la copie enregistrée de l'image dans les documents ou la galerie de photos du téléphone. OU coller l'URL de l'image dans la barre de recherche TinEye.

3 Sélectionner l'une des images renvoyées puis basculer entre « Votre image » et « Image correspondante »

*Ce guide propose des solutions à titre indicatif, certaines solutions peuvent être soumises à conditions



Recherche d'image inversée GOOGLE

Google image met à disposition une solution de recherche d'image inversée permettant de savoir quand l'image a été utilisée pour la première fois et où et quand l'événement qu'elle représente s'est produit. Il aide également à vérifier si l'image provient d'une source crédible.

1 Enregistrer ou télécharger la photo à vérifier. On peut également copier l'adresse Web de l'image que l'on souhaite vérifier. Attention : Cela doit être l'URL de la photo réelle, pas de la page Web entière.

2 Accéder à https://images.google.com.

3 Se rendre dans le menu du navigateur, faire défiler vers le bas et sélectionner « Demander le site du bureau ». Dans Google Chrome, le menu est trouvé en appuyant sur les trois points en haut à droite de l'écran. Dans iOS Safari, c'est au centre en bas de l'écran.

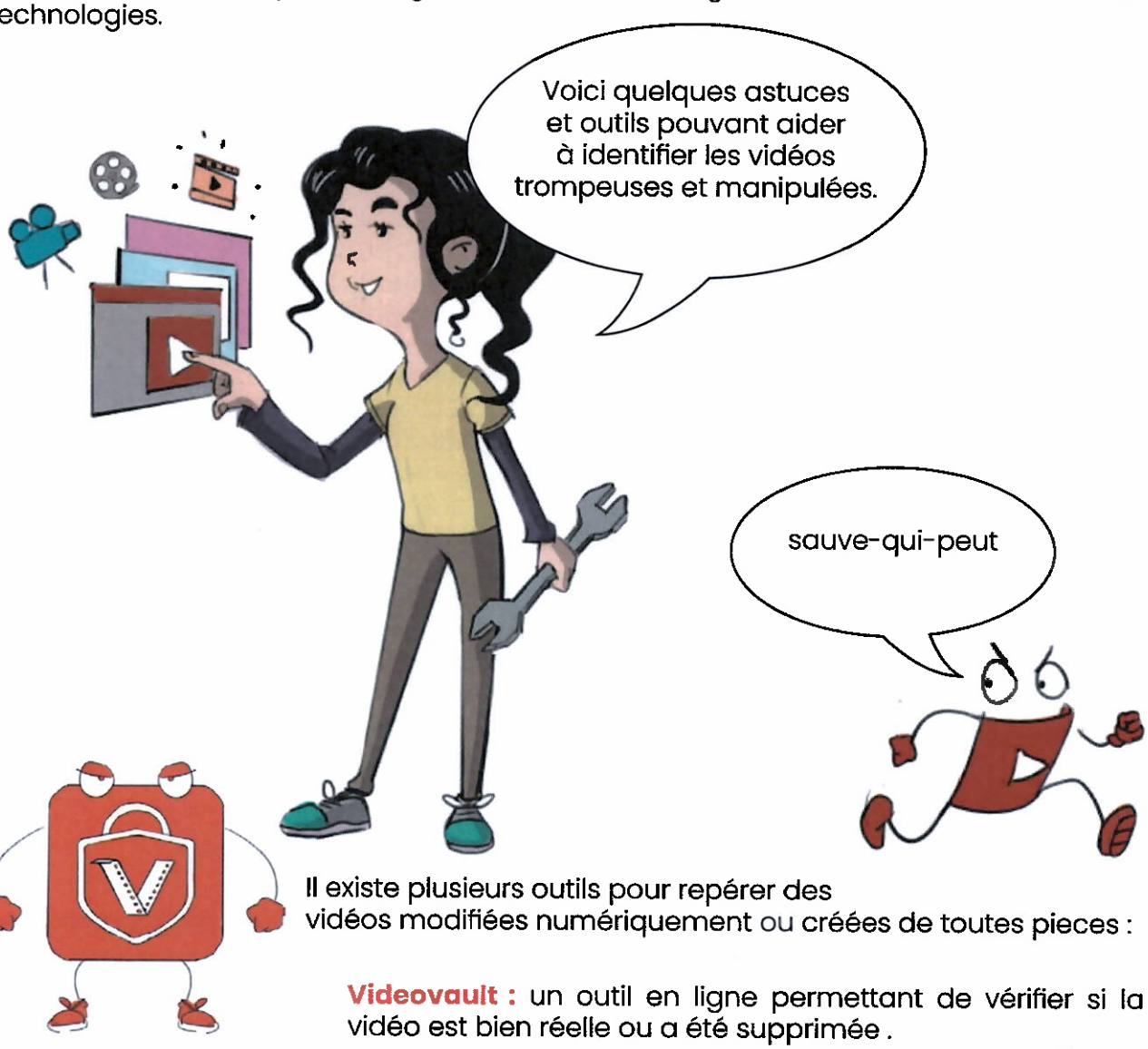
4 Appuyer sur l'icône de l'appareil photo dans la barre de recherche.

5 Deux options se présentent. Soit coller l'URL de la photo à vérifier dans la barre de recherche. Soit sélectionner l'onglet « télécharger une image » pour télécharger l'image à partir de l'endroit où elle a été enregistrée sur le téléphone.

6 Vérifier les résultats pour savoir quand et où l'image a été utilisée. Si l'on retourne loin en arrière, on devrait être en mesure de trouver où elle a été utilisée pour la première fois, éventuellement, le propriétaire du droit d'auteur de l'image.

Comment déceler des vidéos trompeuses, hors contexte et en mode " DEEPFAKE "

Les vidéos peuvent être créées de toutes pièces ou manipulées avec talent pour induire en erreur. Elles peuvent également être créées grâce à l'utilisation des nouvelles technologies.



Il existe plusieurs outils pour repérer des vidéos modifiées numériquement ou créées de toutes pieces :

Videovault : un outil en ligne permettant de vérifier si la vidéo est bien réelle ou a été supprimée .

YouTube DataViewer : outil en ligne développé par Amnesty International .Il permet de vérifier l'origine d'une vidéo YouTube.

Kapwing : outil gratuit en ligne qui permet de vérifier si la vitesse de lecture de la vidéo a été manipulée. Lien pour le guide d'utilisation , cliquez ici : https://www.kapwing.com/

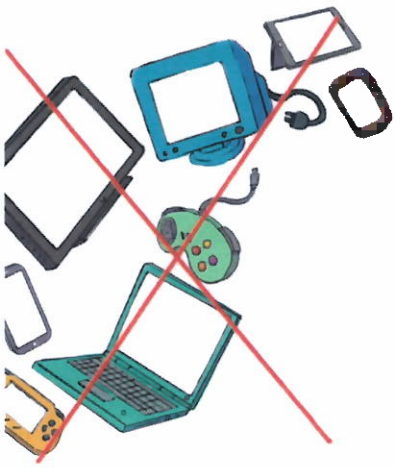
*Ce guide propose des solutions à titre indicatif, certaines solutions peuvent être soumises à conditions

Recommandations

Au Maroc, Internet fait partie du quotidien de la grande majorité de la population. Dans le contexte de crise sanitaire et des transformations que celle-ci a généré sur nos modes de vie, les usages du Net se sont considérablement accélérés et démultipliés.
Notre univers quotidien est dominé par les images, les sons, les mots qui participent à notre éducation civique, citoyenne à développer nos savoirs et notre ouverture sur le monde. En décrypter le sens et la portée, la véracité doit faire partie des apprentissages tant pour les adultes que pour les jeunes publics. Comme nous l'avions déjà indiqué en guise de préambule, loin de diaboliser Internet, ce guide doit au contraire permettre de réconcilier, y compris les plus réfractaires d'entre nous avec cet outil de communication et d'information, et de permettre au plus grand nombre d' y adhérer avec sérénité grâce à des outils adéquats qui facilitent une navigation en toute responsabilité et accompagnent grâce à des repères, les plus jeunes et plus vulnérables dans le monde numérique.

C'est pourquoi, bien au-delà de mises en garde, il est articulé autour de recommandations que nous synthétisons ci-après car c'est sur la mise en pratique de celles-ci que repose la solution pour une navigation sécurisée et responsable.

En matière d'exposition aux écrans des enfants, il est préconisé ce qui suit :



-Pas d'écrans pour les enfants de moins de deux ans ;

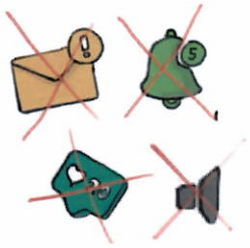
-Pas plus d'une heure quotidienne devant les écrans (télévision ou jeux sur écrans) pour les enfants de plus de 2 ans. Selon les nouvelles directives de la santé des jeunes enfants publiées par l'Organisation Mondiale de la Santé en 2019, l'âge de bannissement total des écrans est fixé à deux ans. Certains préconisent même d'éradiquer les écrans avant l'âge de 3 ans ;

-La lecture d'histoires et les exercices physiques sont recommandés ;

-Le contrôle parental du temps d'utilisation et de la nature et les durées de connexions des enfants demeurent une obligation pour une utilisation saine et sans danger.

-Ensuite, au-delà des contingences cognitives liées à la petite enfance, la superexposition aux écrans constitue un danger tant pour les enfants que pour les adultes. Une régulation du temps d'écran pour tous s'impose.

Afin de prévenir l'addiction numérique des enfants :

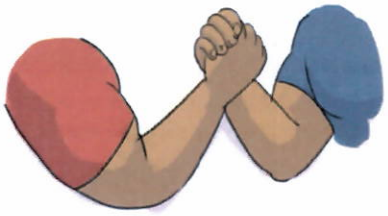


-L'exemplarité des parents constitue un préalable ;

-La désactivation des notifications permet d'éviter de consulter son écran dès qu'une alerte est signalée ;

-L'instauration de zones sanctuarisées sans écrans dans la maison permet de réduire le temps d'écran.

Recommandations en matière de prévention des challenges dangereux :



-Veiller à ce que votre enfant soit en âge de s'inscrire sur les réseaux sociaux ou dispose de la maturité nécessaire ;

-Informer sur les dangers d'un challenge est une démarche essentielle ;

-S'informer aussi pour rester en alerte par rapport aux derniers défis numériques ;

-Suivre par l'historique des moteurs de recherches consultés par l'adolescent.

Recommandations en matière de fact-checking :

-Identifier l'auteur du message ;

-Adopter le principe qu'une information donnée sur le Web par un inconnu est par défaut plus fausse que vraie ;

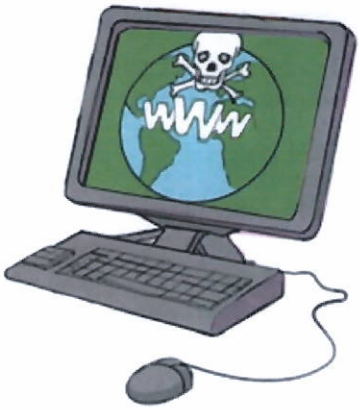
-Recouper le message, une fois la source identifiée en allant consulter des sources d'informations officielles ; agences de presse ; journaux d'information pour vérifier si l'information est relayée par d'autres médias ;

-Remonter à la première source dans la mesure du possible ;

-Utiliser les moteurs et différents outils, de plus en plus nombreux qui aident à vérifier l'information (Africa Check ; les décodeurs ; la rubrique fact-checking de media 24 ; la rubrique desintox du desk.ma) ;

-Il faut toujours se dire que plus une information est surprenante, plus elle doit être étayée et précise.

Recommandations en vue de protéger votre enfant des prédateurs du net :



Outre le contrôle parental, il est essentiel de nouer un dialogue permanent avec ses enfants et de les disculper, les mettre à l'aise afin qu'ils puissent se confier dès lors qu'ils se retrouvent face à des contenus inappropriés.

Parmi les nombreux outils, le CPS (Child Protection System) est un logiciel mondial pour lutter contre les abus d'enfants.

Recommandations pour protéger vos données personnelles

Toutes les informations que je poste sur youtube facebook ou autres plateformes sont réutilisées. Les conditions générales d'utilisation des sites fréquentés expliquent comment nos données sont réutilisées. C'est pourquoi il est important d'en prendre connaissance.
L'utilisation d'avatars et de pseudonymes permet de renforcer la protection de sa vie privée. Avant de publier une information, il importe de s'assurer qu'elle ne nuit ni à sa propre réputation, ni à celle d'autrui, ni à la loi et de vérifier la véracité de l'information publiée.
Il existe un référentiel international sur la protection des données.

Table des matières

Les auteurs

Responsable éditoriale : Narjis Rerhaye, présidente du groupe de travail, membre du Conseil Supérieur de la Communication Audiovisuelle,

Rédacteurs : Latifa Tayah, Amine EL Bouazzaoui, Direction générale de la Communication Audiovisuelle,

Maquettiste et illustrateur : Hamza Tamouh, Direction générale de la Communication Audiovisuelle,

Révision : Oumaima EL Khattabi, secrétaire du groupe de travail « Régulation et médias numériques »

Contact

E-Mail : info@haca.ma

Tél: +212 5 37 57 96 00

Fax: +212 5 37 71 42 74

Site web : www.haca.ma

Espace Les Palmiers, Lot 26,
Angle Avenue Annakhil et Mehdi Ben Barka, B.P
20590-Hay Ryad-Rabat-Maroc

الهيئة العليا للاتصال السمعي البصري

ⵓⵔⵔⵓ ⵓⵎⵙⵙⵓⵔ ⵏ ⵜⵎⵔⴰⵡⵉⵙ ⵓⵖⵏⵉⵎⵓⵙ

Haute Autorité de la Communication Audiovisuelle

www.haca.ma