ⵜⴰⴳⵍⴷⵉⵜ ⵏ ⵍⵎⵖⵔⵉⴱ
ⵜⴰⵎⴰⵡⴰⵙⵜ ⵏ ⵜⵣⵔⴼⵜ
ⴷ ⵜⴷⵍⵉⵢⴰ ⴷ ⵜⵙⵙⵓⵎⵙⵉ

المملكة المغربية
وزارة الشباب
والثقافة والتواصل

Royaume du Maroc
Ministère de la Jeunesse, de la Culture et de la Communication

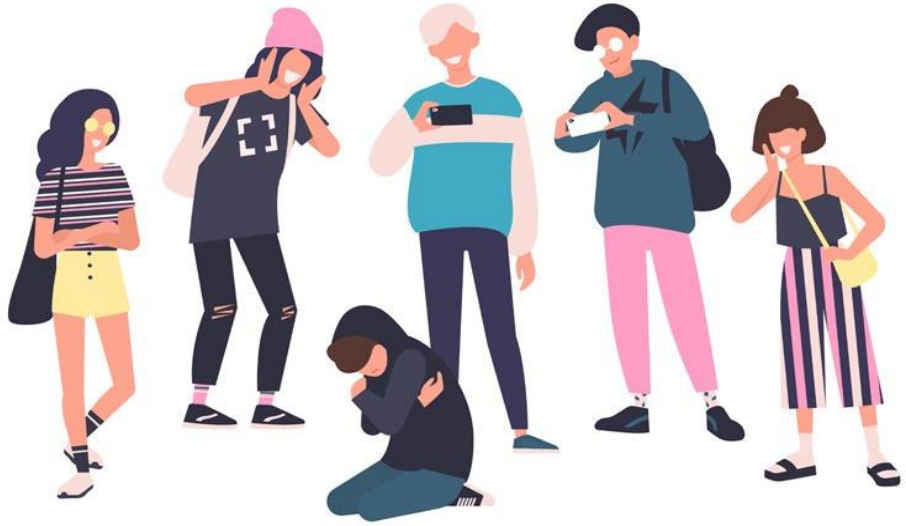
Financé
par l'Union européenne
et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Mis en œuvre
par le Conseil de l'Europe

CMRPI
Centre Marocain de Recherches
Polytechniques et d'Innovation



Ateliers de formation-pilote

Département de la jeunesse - Région de Casablanca-Settat

Implantation d'équipes ressources dédiées au traitement des situations de cyberviolence et du cyberharcèlement chez les jeunes

Bouznika, février 2023

Mini-biographie:

- **Enseignant-chercheur**, en mathématiques et informatique, Université Ibn Tofail, ENSA-Kénitra, Maroc.
- **Président fondateur du CMRPI**, www.cmrpi.ma, (depuis 2012).
- **Expert du conseil de l'Europe** en cybersécurité et protection des enfants dans l'environnement numérique
- **Directeur de la Campagne Nationale de lutte contre la cybercriminalité au Maroc**, CNLCC- 2014-2017.
- **Coordonnateur du comité national Safer Internet Day-Morocco**, journée mondiale pour un Internet sûr, depuis 2018.
- **Directeur de Espace Maroc Cyberconfiance**, www.cyberconfiance.ma depuis 2020
- **Ex- commissaire judicaire de deuxième grade**, administration centrale du Ministère de la Justice, (10 ans d'expérience).

Module 1
Cyberviolences, risques en ligne, facettes techniques

Chapitre 1

Facettes techniques de cybercriminalité chez les enfants et les jeunes

Internet est formidable, mais attention !

Internet est un monde merveilleux pour tout le monde ! plein d'avantages :

- Moyen de communication
- Moyen d'apprentissage
- Moyen de divertissement
- Moyen d'épanouissement
- etc.

La crise Covid a démontré par l'exemple son intérêt

Malgré les multiples avantages d'internet,

il présente des risques potentiels ! à savoir les multiples facettes de la cybercriminalité

Avec dégâts humains et économiques estimés à **600 milliard de dollars**, soit 50 fois le PIB du Maroc, ou soit près de deux fois le PIB de la France.

La cybercriminalité est devenu un monstre.

Malgré les multiples avantages d'internet, il présente beaucoup de risques ! à savoir la cybercriminalité

Actuellement, les cybercriminels profitent des possibilités d'internet : **anonymat, chiffrement, cryptographie**, mais aussi des nouvelles technologies, pour mieux s'organiser, il ne s'agit plus uniquement des simple **hackers (amateurs)**, mais ce sont souvent **des groupes bien organisés**, dotés des dernières technologies.

Les risques de la cybercriminalité est en évolution

Malheureusement, l'ensemble des avancées scientifiques sont exploitées par les cybercriminels.

Sans pouvoir les identifier, les cybercriminels peuvent désormais utiliser l'Intelligence Artificielle, notamment le « Machine Learning » pour **exploiter les enfants et les jeune, ainsi les manipuler.**

L'avenir de l'intelligence artificielle (IA) cache encore des surprises pour la sécurité en ligne.

Complexité de la cybercriminalité : non maîtrisable

Aujourd'hui on maîtrise moins de 10% du trafic d'Internet

- **Web surfacique** (Surface Web)

C'est notre quotidien sur Internet, consultation des courriels, connexion aux réseaux sociaux, achats en ligne, etc. ce sont des sites indexés par les moteurs de recherche.

- **Web profond** (Deep web : web caché)

Estimé à 70 ou 75% du web total, c'est l'Internet de tous les **contenus qui ne sont pas indexés** par les moteurs de recherche.

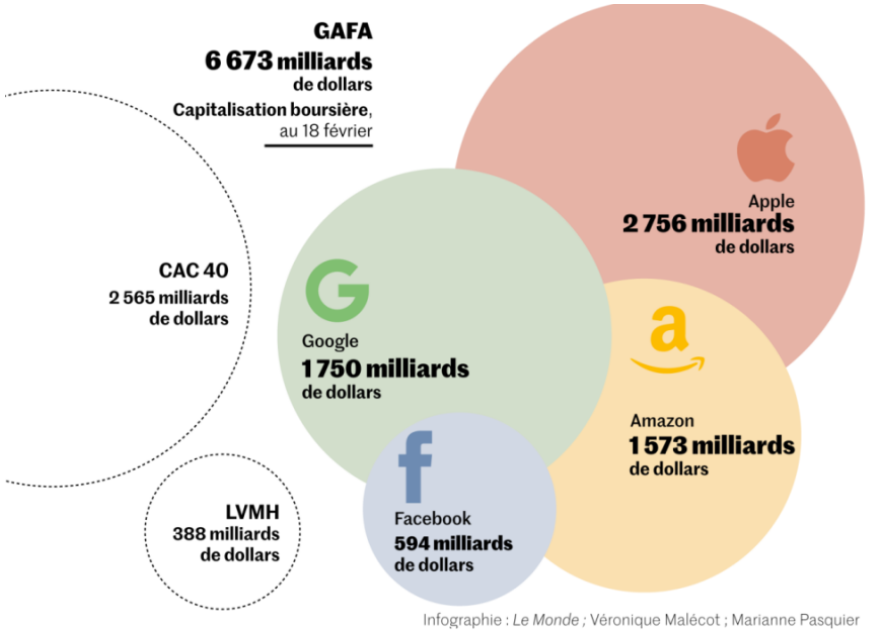
- **Web sombre** (Dark web)

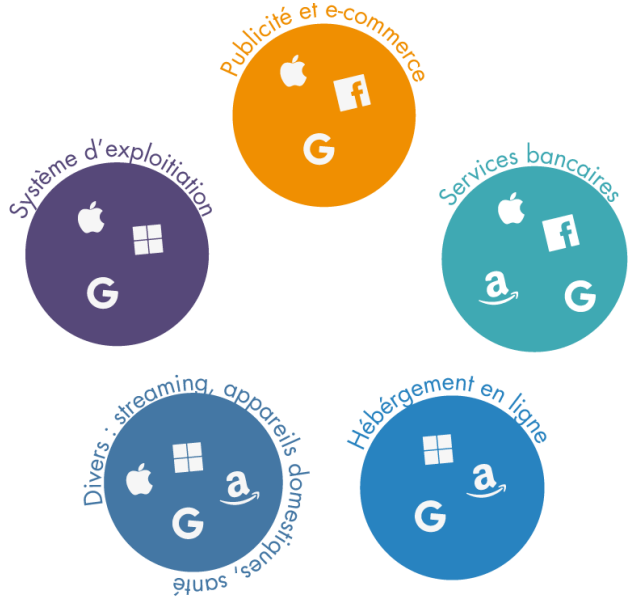
Non connu par les moteurs de recherche : vente de cartes bancaires, armes, drogues, contrefaçons, **pédopornographie**, embauche de tueurs, transport et ventre d'organes, achats de logiciels malveillants, etc.

Monopole de l'internet

Le 10% du web de surface qu'on maitrise aujourd'hui, est monopolisé par les géants de l'internet, à savoir les GAFAM :
Google, Apple, Facebook (Meta), Amazon, Microsoft,
En plus du nouveau gênant chinois émergent BATX

Les Géants d'Internet constituent une puissance économique technologique, Ils peuvent même influencer les politiques





Contrôlent le trafic du web et détiennent la technologie et les infrastructures

- Environ **95%** de câbles sous-marins reliant les quatre coins de la planète;
- Environ **80%** des données mondiales sont localisées dans des datacenters américains, au Silicon Valley, en Californie

Cybersécurité et protection en ligne / collaboration avec les géants de l'internet

Toute stratégie de cybersécurité et de protection en ligne,, doit impérativement passer par une collaboration avec les géants d'internet

"Celui qui détient l'information, détient le pouvoir, celui qui l'entretient, détient le monde "

Citation célèbre d'Adam Smires, philosophe

Les géants d'internet détiennent l'information (datacenters) et l'entretien (Data analysis, Big data)

.

Lutte contre la cybercriminalité : multi-dimensions

- **Dimension technique**

Infrastructures et équipements sécurisées

- **Dimension juridique**

Textes de loi évolutifs et actualisés

- **Dimension organisationnelle**

Institutions spécialisées et efficaces sur le terrain

Mais surtout aussi la sensibilisation aux risques et aux bonnes pratiques d'usage sécurisé d'internet, une grande partie des attaques cybercriminelles sont à la base des failles humaines.

Protection des enfants et des jeunes en ligne

Aujourd'hui, les enfants et les jeunes, comme le cas des adultes, sont exposés aux multiples facettes de cybercriminalité, avec beaucoup plus de risques vue leur :

1. **Vulnérabilité**
2. **Présence fréquente dans l'espace du numérique**

Ceci complique la mission de leur protection sur internet.

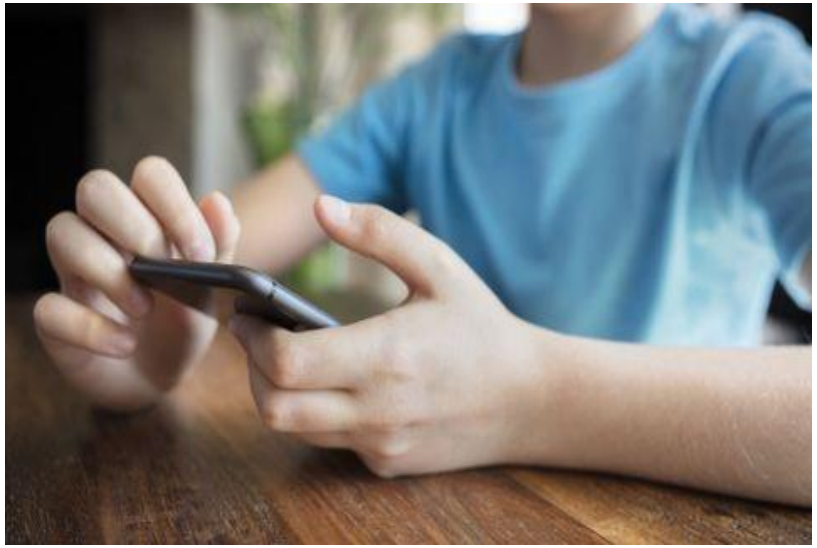
Protection des enfants et des jeunes en ligne

les jeunes, surtout les enfants sur internet ont besoin :

- **d'une protection particulière lorsqu'ils sont en ligne**
- **doivent être accompagnés pour apprendre à éviter les dangers**
- **doivent avoir un traitement spécifique, si jamais il sont victimes de cybercriminalité.**

Protection des enfants et des jeunes en ligne

- Protéger les enfants en ligne, **c'est comprendre les différentes facettes techniques et comportementales qui représentent un risque ou une menace** dans l'environnement numérique.
- Anticiper les **risques émergents** (**via Intelligence artificielle par exemple, qui permet d'analyser le comportement des enfants et jeunes en ligne**, en exploitant leurs données personnelles)



Cartographie des risques numériques chez les enfants et les jeunes

- Pour simplifier, on peut se baser sur les lignes directrices de l'Union International de Télécommunication UIT, (2020), sur la protection en ligne des enfants
- Les risques numériques que recours les enfants en ligne peuvent êtres classées par catégories :

✓ **Catégorie 1 : Contenu et manipulation**
✓ **Catégorie 2 : Contact avec des adultes ou d'autres enfants**
✓ **Catégorie 3 : Logiciels et matériel**

Principales facettes de violence en ligne chez les enfants et les jeunes

Exposition à **des contenus inappropriés**, **violents**, **pornographique**, **publicitaires racistes**, ou de **haine**
(L'enfant peut être **victime ou auteur**)

Conséquences

Réactions extrêmes : automutilation (Blessures, suicide), des comportements destructeurs et violents, radicalisation ou adhésion à des idées racistes ou discriminatoires.

Principales facettes de violence en ligne chez les enfants et les jeunes

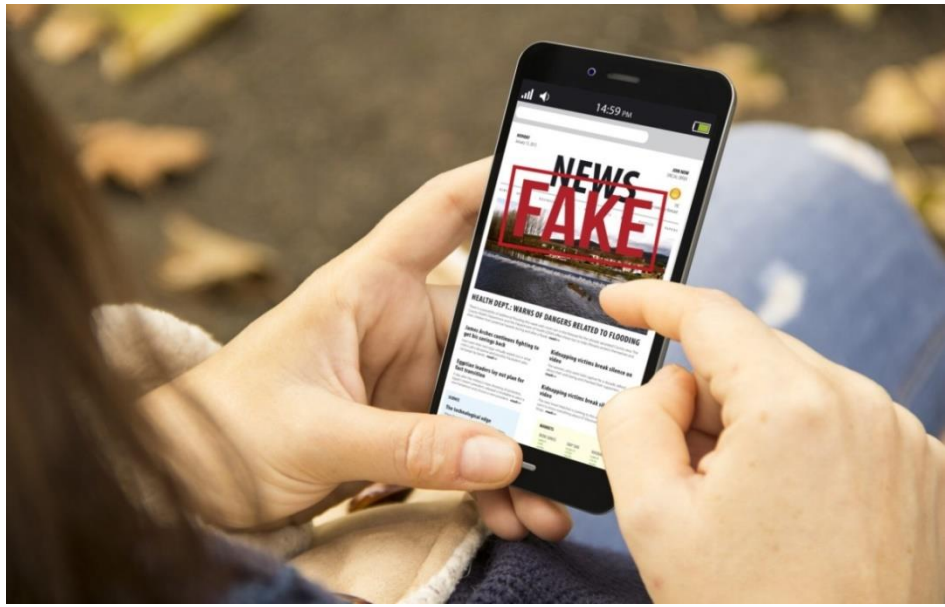
Actes de **cyberintimidation et d'exploitation sexuel en ligne** (publication de photos ou vidéos intimes), pour des raisons multiples: racistes, religieuses, ou même prolonger le mal causé dans la vie réelle vers la vie virtuelle.

Conséquences

Tristesse, solitude, insomnie, perte de confiance en soi, absentéisme à l'école… une situation douloureuse qui peut conduire à la **dépression.**

Principales facettes de violence en ligne chez les enfants et les jeunes

Exposition **à des fausses informations**, **désinformation** ou informations inexactes ou incomplètes



Conséquences

Les enfants et les jeunes peuvent adopter une **vision déformée du monde**.

Principales facettes de violence en ligne chez les enfants et les jeunes

- **Grooming** (toilettage en français) **:** manipulation psychologique par un adulte à des fins sexuelles, **construire une relation intime et émotionnelle avec un mineur**.
- C'est une nouvelle pratique faite à travers les **réseaux sociaux, les forums de discussion, les sites de jeux vidéo**, pour prendre contact avec un enfant afin d'obtenir des actes sexuels (via une webcam par exemple) ou afin de le rencontrer hors ligne pour abuser de lui sexuellement.
- Le cybercriminel, pour mieux gagner la confiance de sa victime **se fait passer lui- même pour un enfant.**

Principales facettes de violence en ligne chez les enfants et les jeunes

Sexting: consiste à envoyer des messages, photos ou des vidéos sexuellement explicites par SMS (on parle aussi de sextos), messageries ou chats.

C'est une activité pratiquée principalement par les adolescents;

On distingues deux types:

- **sexting primaire**

Lorsqu'une personne diffuse elle-même un contenu, vidéo ou photo la représentant, dans un cadre qui se veut privé.

- **sexting secondaire:**

Lorsqu'un individu transfère le matériel qu'il aura reçu ou produit d'une tierce personne.

Principales facettes de violence en ligne chez les enfants et les jeunes

- **Sextorsion**: **chantage à la web cam**, quand un internaute menace de partager une photo ou une vidéo intime.

Actuellement, une nouvelle forme de chantage :

- A l'aide des logiciels de retouches d'images le cybercriminel superposent des visages de jeunes personnes ou enfants sur des vidéos ou des photos pour faire croire qu'elles sont nues ou se livrent à des actes sexuels.

Principales facettes de violence en ligne chez les enfants et les jeunes

Diffamation et atteinte à la réputation

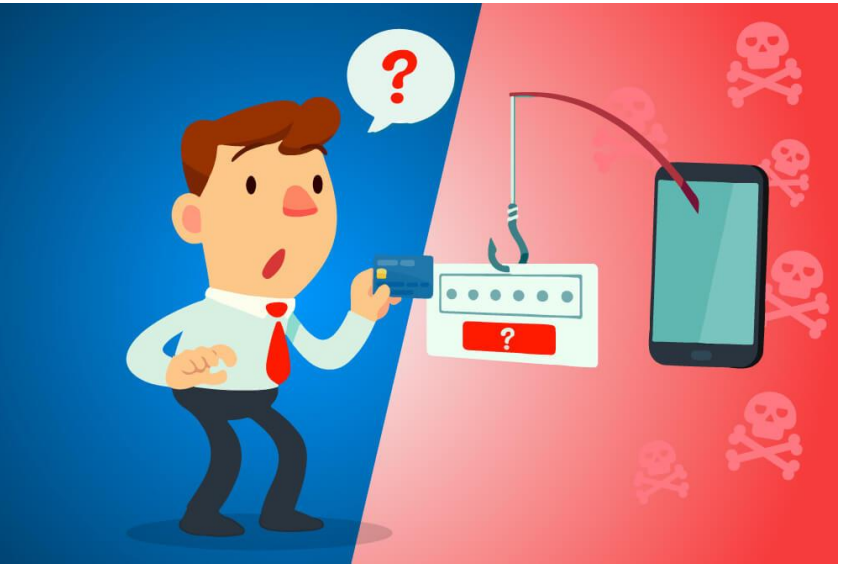
Lorsqu'une personne **publie sur internet des propos désagréables à l'égard d'un tiers** tout en les sachant faux (ou même vraies), avec l'intention de nuire à autrui.

Principales facettes de violence en ligne chez les enfants et les jeunes

Usurpation d'identité

- Désigne l'utilisation d'informations personnelles d'une personne sans son accord pour réaliser des actions frauduleuses.
- En pratique, ces informations peuvent être obtenues par les cybercriminels par le biais d'un message d'hameçonnage (**phishing**), par le **piratage d'un de ses comptes** en ligne ou d'un de ses appareils ou encore le **piratage d'un site Internet sur lequel ces informations** étaient enregistrées.

Vol de données par techniques phishing



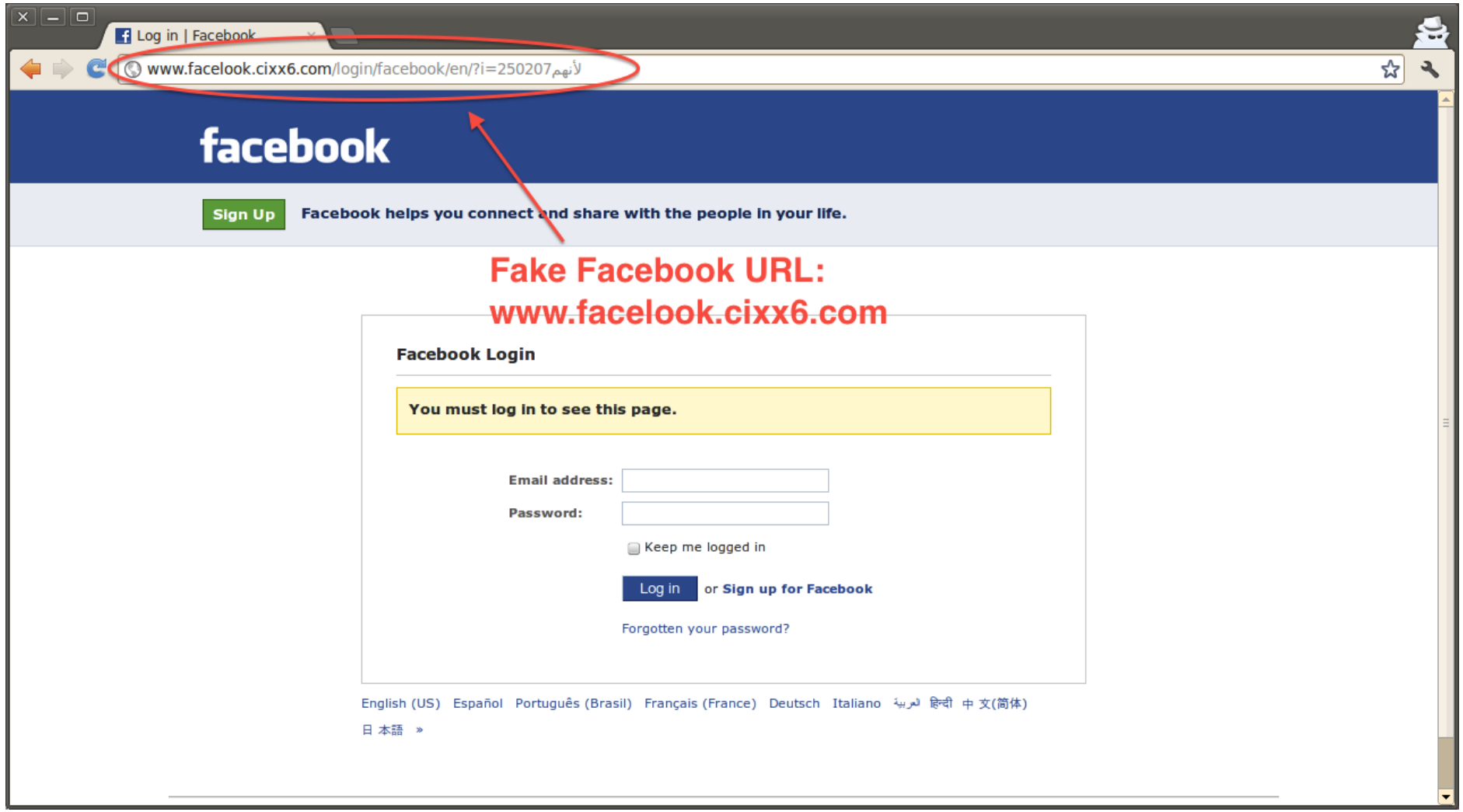
Phishing ou Hameçonnage

Technique de piratage des données (arnaque) destinée à récupérer des informations personnelles, en incitant les enfants à communiquer leurs identifiants et mot de passes.

Comment ça marche (exemple) ?

1- Le pirate fait une petite recherche sur internet de l'adresse mail de la victime.
2- Il envoi un mail à la cible, en lui demandant par exemple de mettre à jours ses renseignements, pour des raisons de maintenance technique de l'application ou pour raison de migration de serveurs.
3- La victimes est renvoyée vers une fausse page web, **très similaire à l'originale**, pour introduire l'identifiant et le mot de passe.
4- le cybercriminel récupère ensuite le mot de passe et le change.

Vol de données par techniques phishing



(URL :adresse de la page web n'est pas conforme)

Arnaque et chantage à la webcam

Comment ça marche (exemple) ?

- Recevoir un message (email) d'un supposé pirate anonyme ou « hacker » qui prétend avoir piraté votre compte mail et accédé à votre smartphone.
- Il vous menace de publier des photos prétend prendre à votre insu avec votre webcam et vous demande une rançon en monnaie virtuelle.

Arnaque et chantage à la webcam

Explications (trois cas possibles)

1- Le cybercriminels peut toujours **masque l'adresse de l'émetteur** : l'adresse mail n'est qu'un simple affichage qui peut facilement être usurpé (masqué)

2- Le cybercriminel peut avoir vote mot de passe : de nombreux sites, parfois très réputés, se font régulièrement pirater leurs bases de comptes utilisateurs (les mots de passes se vendent dan le marché noire)

3- Le cybercriminels a vraiment réussi à pirater votre mot de passe (par technique de phishing)

Malheureusement, les victimes ne changent pas assez souvent leurs mots de passe

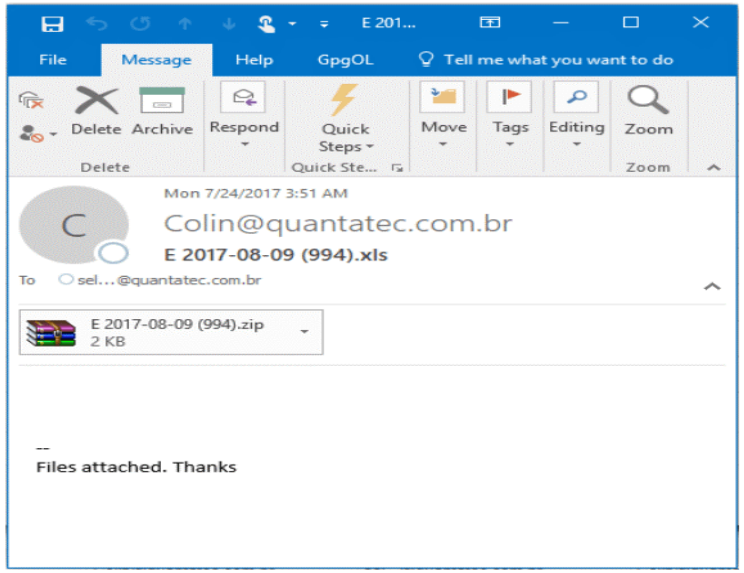
Ransomware et chiffrement des données

Le ransomware (ou rançongiciel), virus informatique qui chiffre (cryptage) les fichiers de la machine (PC, smartphone, tablettes, serveurs, etc.)

Il peut se propager sur le réseau et infecter une série de machines.

Après cryptage, le hacker force la victime à payer une rançon, allant de centaines à plusieurs milliers de dollars, sous forme de monnaie virtuelle (bitcoin)

Ransomware et chiffrement des données



Comment ça marche (exemple) ?

La victime reçoit généralement un mail avec pièce jointe (extension zip, ou jpg (photo), ou autres)

Après téléchargement et ouverture de la pièce jointe, la machine est infectée et les fichiers sont cryptés.

Le pirate demande une rançon avec un délai entre e 24 à 48 heures, sinon la rançon sera majorée.

En cas d'enfant, il peut voler des cartes bancaires, de l'argent ou des bijoux pour payer la rançon.

Métadonnées des photos publiées risque majeur

Risque des photos publiées en ligne

Les photos prises par des appareils photo numériques peuvent contenir beaucoup d'informations d'identification, telles que **la date**, **l'heure, la marque de l'appareil photo** avec lequel elles ont été prises, **les coordonnées GPS de l'endroit où ils ont été prises**, ce qui présente un risque majeur pour la vie privée des enfants.

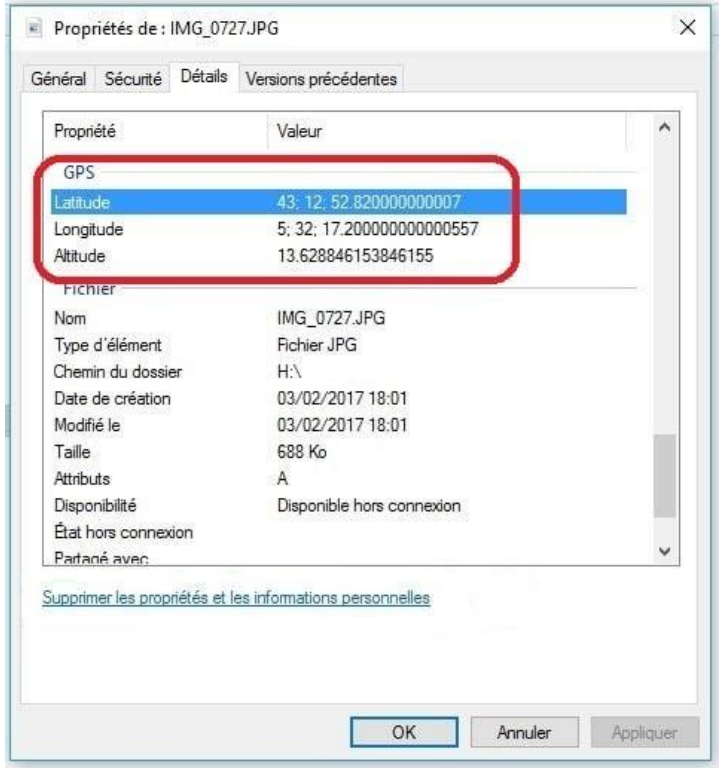
Sans le savoir, un enfant peut révéler à tout le monde où il vit, en publiant une simple photo.

Métadonnées des photos publiées risque majeur

Voici principalement des informations techniques liées au métadonnées que peut contenir une photo publiée sur Internet:

Appareil photo
Marque et Modèle
Date du cliché
Vitesse d'obturation
Exposition
Ouverture du diaphragme
Sensibilité (ISO)
Distance focale
Objectif
Flash activé ou désactivé
Source lumineuse

Identification
Coordonnées GPS
Copyright
Nom de l'auteur
Adresse
Numéro de téléphone
Adresse email
Site web
Licence
Pays où a été prise la photo



Métadonnées des photos publiées risque majeur

La photo numérique est aussi un vecteur d'attaque cybercriminelle

Il est toujours possible d'insérer **un virus** (code), dans les métadonnées d'une photo, grâce à des logiciels gratuit comme 'Exiftool'(**logiciel permettant de lire, écrire et manipuler les métadonnées des images**)

Le code (virus) pourra ensuite être exécuté une fois télécharger (endommager la machine, espionner, prendre le contrôle, activer la Cam et le micro à distance)

Il faut supprimer les métadonnées des photos avant de les partager ou les publier

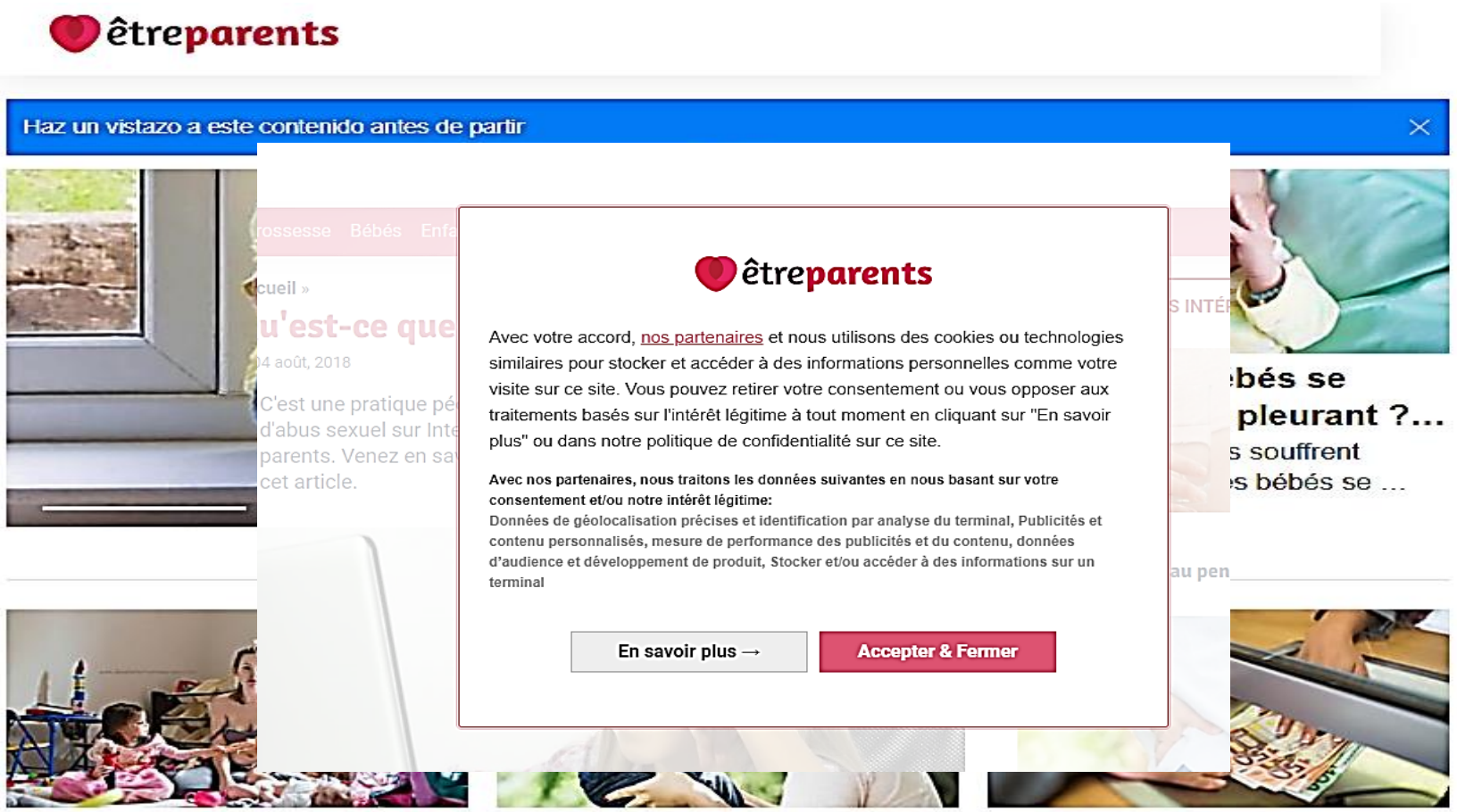
Cookies et espionnage

Les cookies sont des fichier texte utilisés par les sites web pour suivre les activités et préférences d'un visiteur pour des fins de marketing, en principe, la pratique ne vise pas l'espionnage.

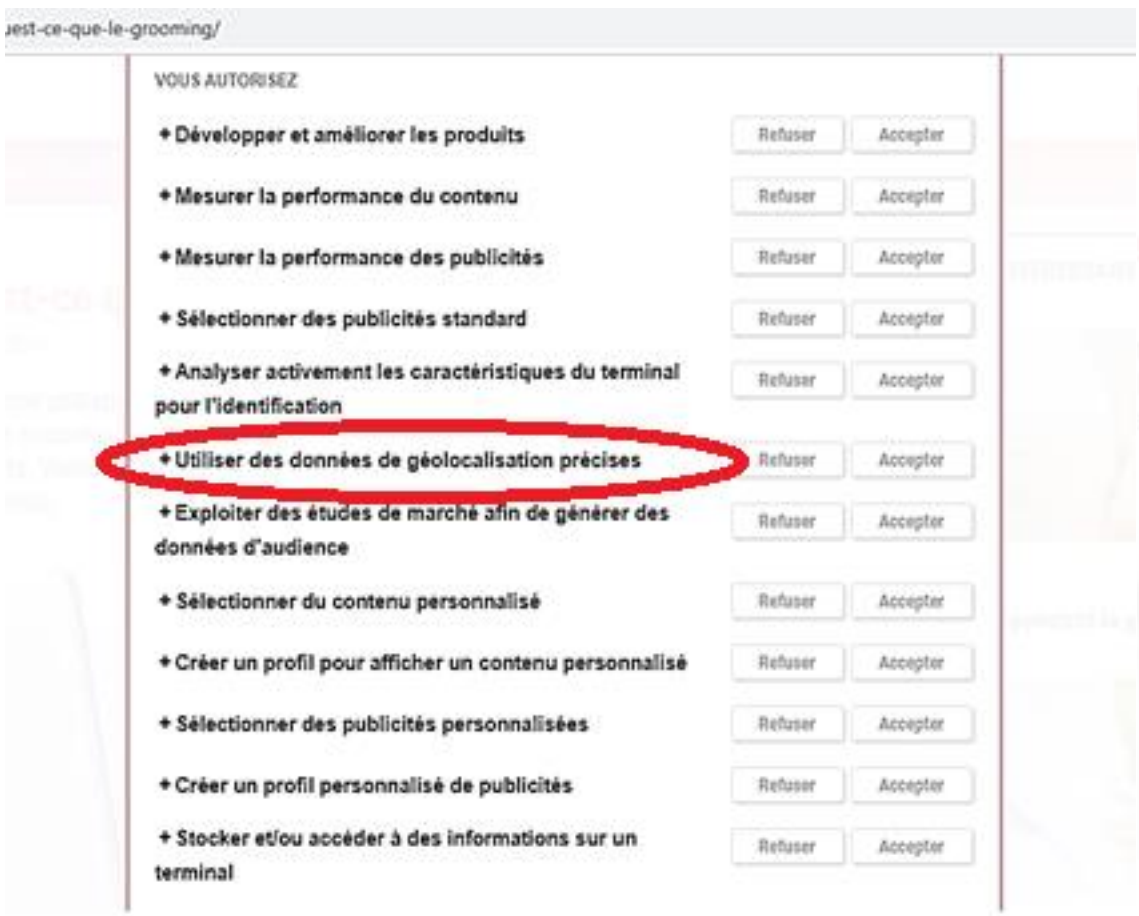
Par contre **les hackers tentent à récupérer les cookies**, l'objectif étant pour eux d'en exploiter le contenu et d'utiliser ces données personnelles à des fins malveillantes.

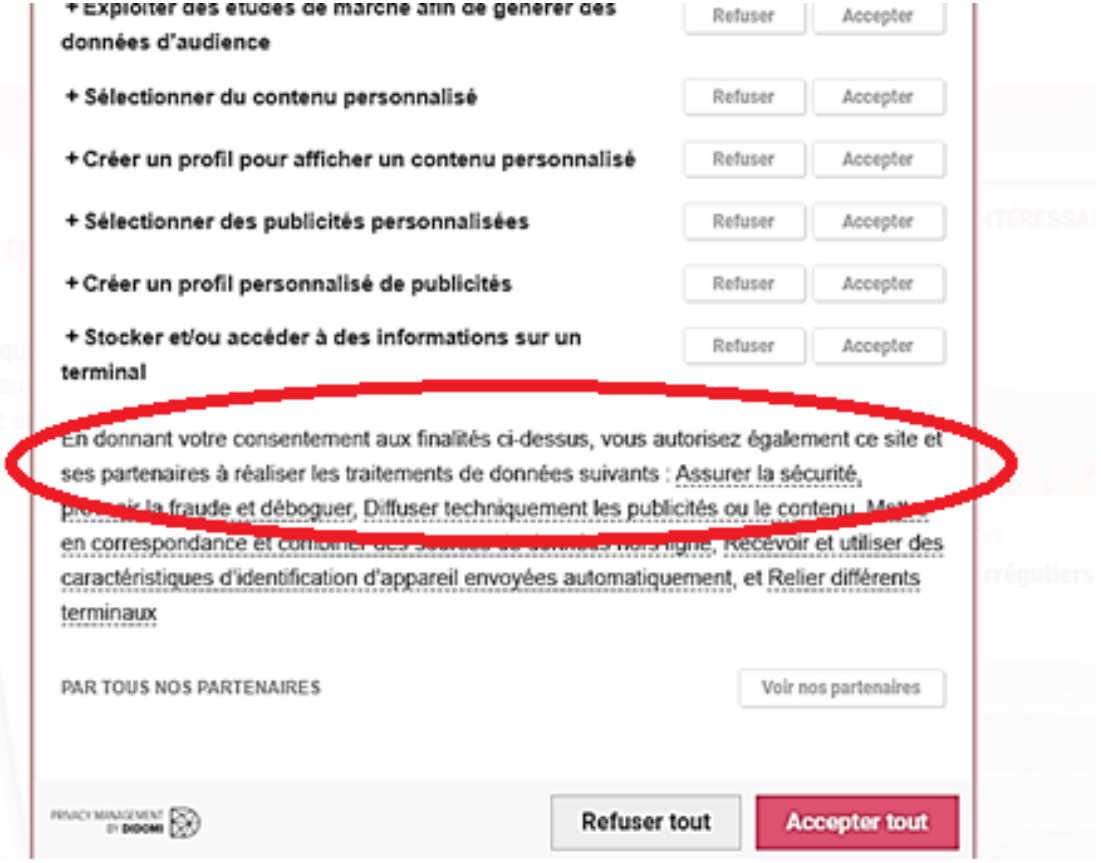
Cookies et espionnage

Exemple:
https://etreparents.com/quest-ce-que-le-grooming/



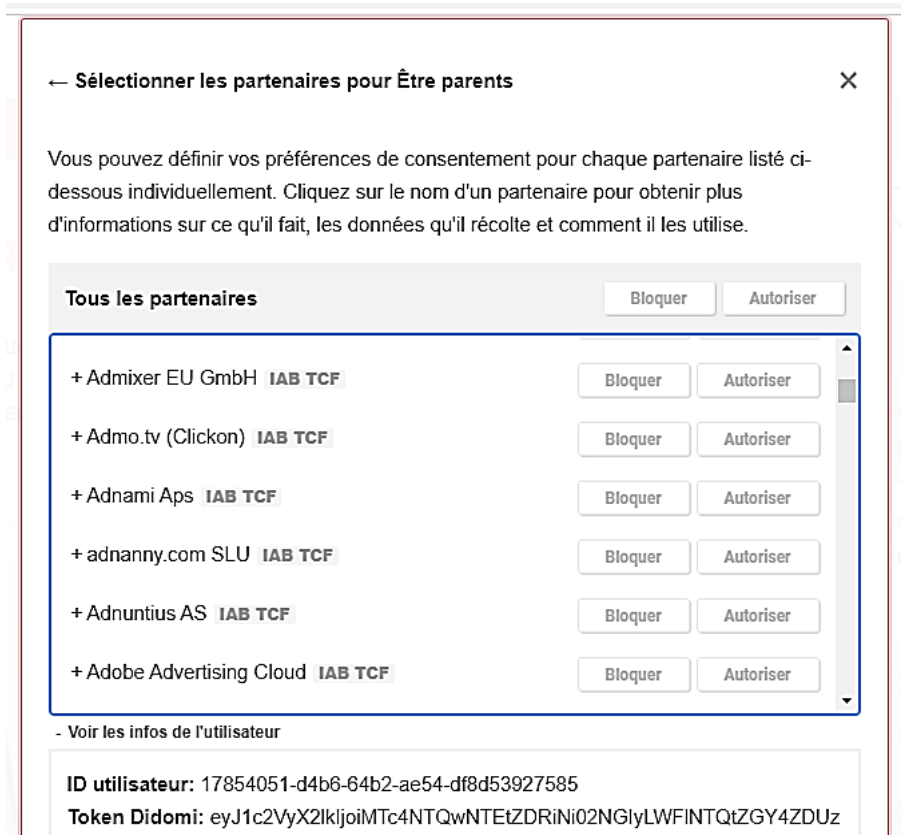
Cookies et espionnage

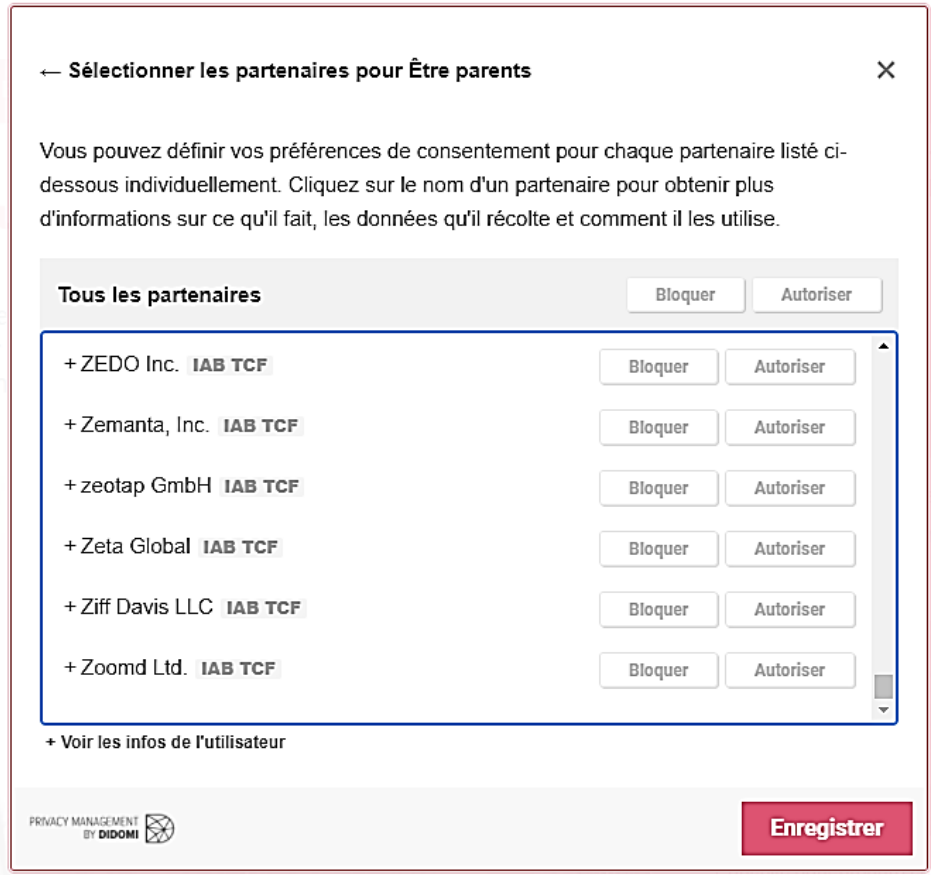




Cookies et espionnage

La liste des partenaires compte au moins une centaine, qui récupèrent les données personnelles des visiteurs du site





Principales facettes de violence en ligne chez les enfants

- **Exploitation des enfants à travers les jeux en ligne** rencontre avec les inconnus ou mêmes des adultes **(Tchat et groupe de discussion)**
- **Risque potentiel d'addiction**

Principales facettes de violence en ligne chez les enfants

- **Dommage matériels ou logiciel**, virus, vers (tablettes, Smartphones, pc, console de jeux)
- **Cookies et espionnage**, **vol des données des enfants**

Nouveaux défis: risque futuristes: l'IOT

D'après une étude de HP sur 10 objets connectés (IOT: Internet of Things) :

(montre, domotique, webcam, etc.)

- 9 objets sur 10 stockent ou communiquent des données personnelles de l'utilisateur
- 7 objets sur 10 ne chiffrent pas les données qu'ils transfèrent vers le réseau
- 8 objets sur 10 ne posent aucune restriction sur le choix du mot de passe, permettant ainsi à l'utilisateur de choisir un mot de passe simple du type « 123456 ».

Que pensez-vous?