
LIVRET ADULTE
(PARENTS ET ENSEIGNANTS)
UN OCÉAN DE DONNÉES
MERCI DE DOUTER AVANT DE CLIQUER!
fleuve des libertés individuelles
APPRENDRE À NAVIGUER EN PRIVÉ
PORT DE L'ARNAQUE EN LIGNE
PHISHING PIRATE
COURANT DU MODE PRIVÉ
TOURBILLON DE LA CYBERVIOLENCE
DÉFENSE DE PÊCHER
KRAKEN DU CYBER-HARCÈLEMENT
PHARO
SUSPECTS
BATEAU DU LIEN SOCIAL
TEMPÊTE DE L'USURPATION D'IDENTITÉ
CHUT! EXPLORE
EXPLORATIONS NUMÉRIQUES
TOUS ENSEMBLE PRUDENCE SUR INTERNET
CNIL
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

SON PREMIER TÉLÉPHONE PORTABLE

Le pitch

→ Devenus des extensions de nos vies physiques, les appareils connectés individuels, ou smartphones, nous permettent d'être en lien constant avec nos familles, amis, collègues ; de produire et consommer des contenus audio, vidéo, photo.

Une opportunité de partage et d'accès à l'information de manière simple et intuitive, que l'on peut emporter partout, tout le temps, avec nous !

INCROYABLE MAIS VRAI !

75 % des parents disent avoir équipé leur enfant d'un téléphone portable entre la 6e et la 3e, à leur initiative et non celle des enfants.

Des raisons liées à la sécurité et l'organisation : pour pouvoir se joindre mutuellement si besoin, parce que les enfants prennent les transports en commun seuls ou encore parce que les activités extra-scolaires sont éloignées du domicile familial.

Les parents équipent aussi les enfants pour qu'ils puissent faire leurs devoirs (ENT).

Enquête CSA pour la CNIL, décembre 2023

On est tous passés par là

→ L'adolescence, c'est le moment de la construction de l'identité, avec les pairs.

Les enfants se détachent peu à peu de leurs parents, les copains prennent plus d'importance dans leur vie. Entre inspiration et validation, les ados grandissent et se construisent entre eux, à l'abri du regard des adultes.

Cependant, les gestes des adultes restent la référence pour les ados.

Ils sont des points de repère, et ce qui est vu, vécu à la maison est reproduit par les ados.

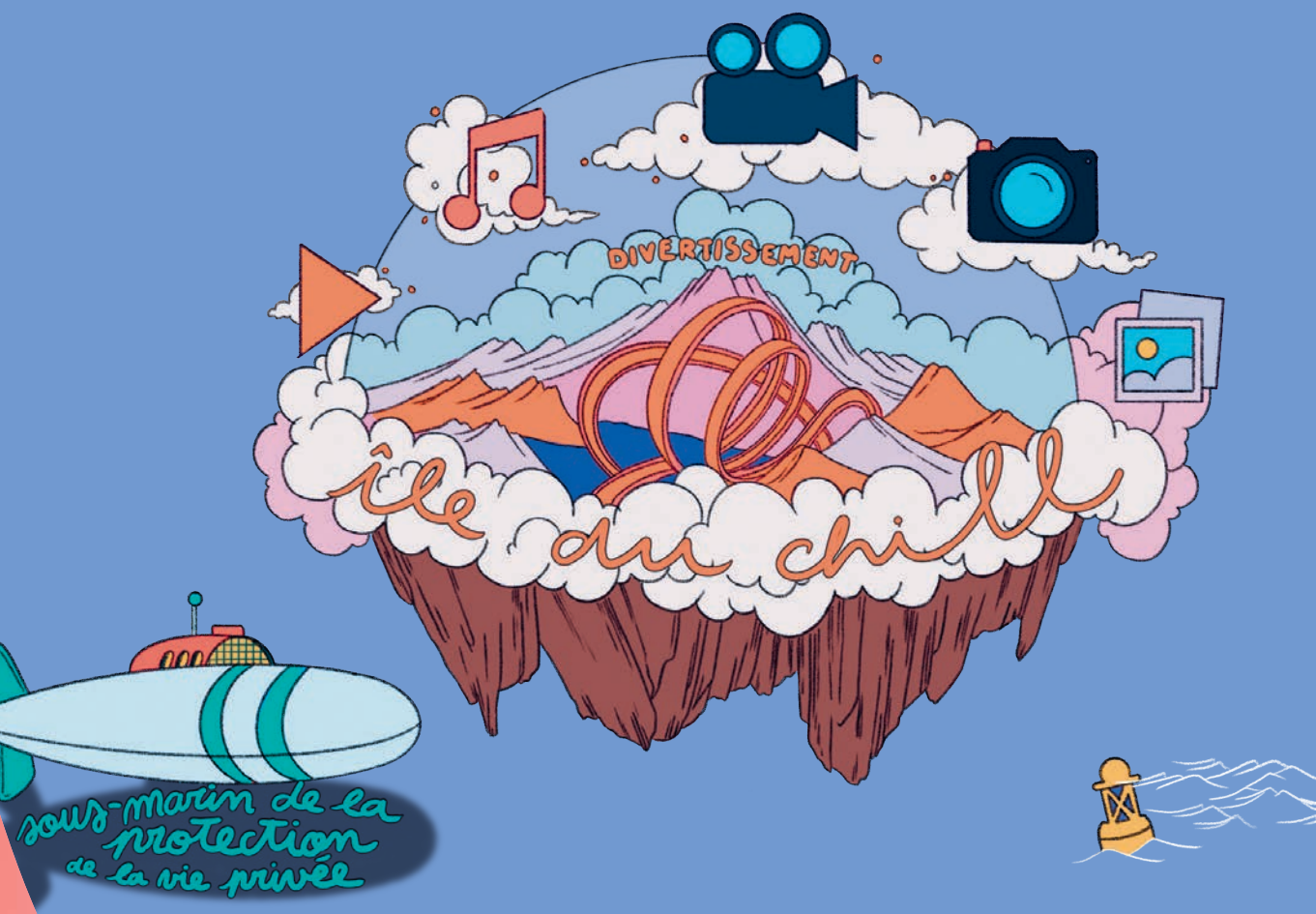
Dans leur vie numérique, les ados font l'objet d'injonctions paradoxales.

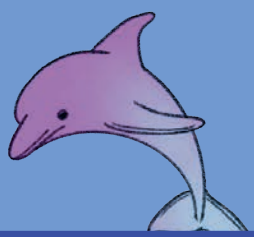
Il faut d'un côté se connecter plusieurs fois par jour pour connaître et faire ses devoirs, et s'insérer dans les groupes de copains, en faire partie. D'un autre côté, on leur reproche leur temps d'écran et on leur demande de se déconnecter alors qu'ils y trouvent une opportunité inédite : acquérir une culture protéiforme (arts, jeux, expression de soi).

POUR EN SAVOIR PLUS

Le Laboratoire d'Innovation Numérique de la CNIL (LINC) a publié ses travaux sur le numérique adolescent :

linc.cnil.fr/numerique-adolescent-et-vie-privee-episode-1-ce-que-dit-la-litterature-en-sciences-sociales





LES CONSEILS

→ Pour accéder à certains contenus et services, il faut s'identifier : fournir une adresse électronique, voire un prénom, un nom, une date de naissance…

Avant leur 15e anniversaire, nous vous recommandons d'accompagner autant que possible vos enfants pour :

- → Créer un compte (ce qui équivaut à signer un contrat).
- → Le paramétrer : préférer le mode privé, désactiver la géolocalisation par défaut…
- → Comprendre ce que signifie « accepter » (notion de consentement) pour certains services en ligne. Exemple : accepter ou refuser les cookies, transmettre des données personnelles à des tiers que l'on ne connaît pas et dont on ne connaît pas les intentions…

ALLÔ, T'ES OÙ ?

Le pitch

→ Aide ou espion, la géolocalisation révèle en temps réel où nous sommes, chaque minute, tous les jours.

La géolocalisation est une technologie qui permet de positionner un objet ou un véhicule sur un plan ou une carte à l'aide de ses coordonnées géographiques. Les positions enregistrées peuvent être :

- stockées au sein de l'appareil,
- extraites ultérieurement,
- transmises en temps réel.

La géolocalisation fonctionne grâce à différents systèmes comme le GPS ou le GSM, les puces RFID, les réseaux wifi ou les adresses IP.

LE CHIFFRE

Environ **30 % des applications** utilisent la géolocalisation, parfois plusieurs fois par minute. Les informations ainsi collectées (lieux visités, horaires…) permettent de déduire des informations sur les habitudes et modes de vie. Si l'on ajoute à cela : le GPS de voiture ou de vélo, la carte de transports ou de péage, le smartphone, et les objets connectés (lunettes, réfrigérateur, vélo, porte-clé, laisse…), s'il est possible de cumuler toutes ces informations alors on peut en déduire où vous habitez, travaillez, faites du sport… à quelle heure vous partez de chez vous, et pour quoi faire.

cnil.fr/fr/maitrisez-les-reglages-vie-privee-de-votre-smartphone

Les idées reçues

→ De plus en plus de familles utilisent la géolocalisation au sein de leur foyer. Pour pister un animal domestique, connaître la position d'un enfant ou d'un sénior. En équipant leurs enfants de téléphone, de montre ou même pour permettre leur géolocalisation en cas de problème, la famille cherche à se rassurer et à se faciliter le quotidien. Une impression souvent illusoire, **engendrant parfois plus d'angoisse :** si l'enfant décide de raccompagner un copain sans avoir prévenu, il s'écarte de son chemin habituel, et là, c'est la panique !

Par ailleurs, c'est la liberté et la relation de confiance qui sont remises en question. **Les enfants ont eux aussi droit à la protection de leur vie privée** et les surveiller en permanence n'est peut-être pas le meilleur moyen de les conduire sur le chemin de l'autonomie.

LES RESSOURCES

Infographie CNIL :

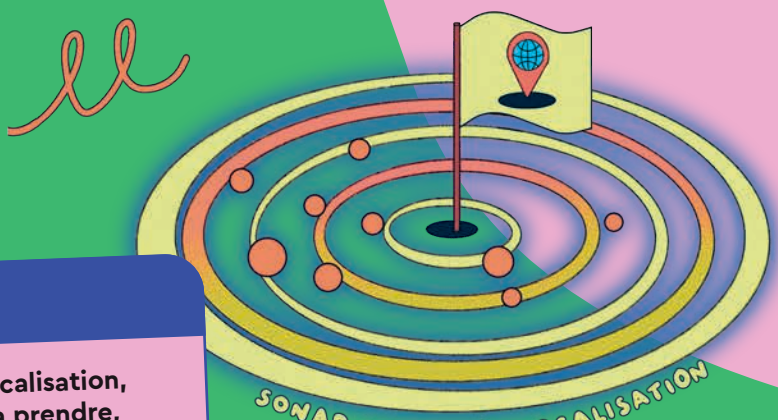
cnil.fr/fr/infographie-il-etait-une-fois-antoine-et-son-smartphone

La vidéo Pix, *Désactiver la géolocalisation* :

tube-numerique-educatif.apps.education.fr/videos/embed/1b0222c7-d659-42ab-be24-90c7deaceba9

ÉLÉMENTS DE CONTEXTE

Internet se nourrit des données personnelles, souvent fournies par les utilisateurs et utilisatrices.
Quand on offre ses données de localisation à tout va, on s'expose à un changement de relation aux autres. On peut avoir des comptes à rendre et souffrir d'un contrôle réel, ou potentiel, permanent, a priori, ou a posteriori. Si vous saviez être géolocalisé(e) en permanence, est-ce que cela changerait vos actions et vos rapports aux autres ?
Nous sommes libres d'aller et venir, et disposons d'un droit à l'intimité !



Réflexes à acquérir

→ S'interroger sur sa géolocalisation, c'est une bonne habitude à prendre, dès le plus jeune âge !

C'est une chance de pouvoir en bénéficier pour s'orienter, trouver son chemin. Mais quand on en a plus besoin, il vaut mieux la désactiver. Donner trop d'informations en partageant ses lieux de vie, de vacances, des photos ou des commentaires peut vous exposer inutilement à des personnes malintentionnées.

CYBERHARCÈLEMENT. COMPRENDRE ET AGIR

Le pitch

→ **Rumeur, piratage, usurpation d'identité, insulte, diffusion de contenus personnels, menaces : le cyberharcèlement peut prendre plusieurs formes.**

C'est avant tout un délit caractérisé par des propos, des comportements répétés qui vont avoir des répercussions négatives sur le physique, le mental, le bien-être de la ou des victimes. Avec des circonstances aggravantes si la victime a moins de 15 ans avec, pour le, la ou les coupables une peine maximale de 3 ans de prison et 45 000 euros d'amende.

- **Insulter quelqu'un en mode privé ou public :** une injure ou une diffamation publique peut être punie d'une amende de 12 000 € (article 32 de la loi du 29 juillet 1881) ;
- **Publier une photo, une vidéo, un vocal sans le consentement de la personne :** pour le non-respect du droit à l'image, la peine maximum encourue est d'un an de prison et de 45 000 € d'amende (article 226-1, 226-2 du code pénal) ;
- **Se faire passer pour quelqu'un d'autre :** l'usurpation d'identité peut être punie d'un an d'emprisonnement et de 15 000 € d'amende (article 226-4-1 du code pénal).

LES CHIFFRES

24 % des familles déclaraient avoir déjà été confrontées au moins une fois à une situation de cyberharcèlement.

Étude Association e-enfance / 3018 / Caisse d'Épargne 2023

Les idées reçues

→ **Le cyberharcèlement dépasse Internet et les réseaux sociaux.**
Ce phénomène de violence est maintenant hybride, aussi influencé par les situations de la vie réelle : vie quotidienne, sorties, vie scolaire, flirt... Le harcèlement peut donc se dérouler dans des espaces publics et privés avec une vraie continuité entre les espaces numériques et physiques.

À l'aide !

→ **En cas d'urgence :** appeler le **17** (fixe ou mobile) ou le **112** (fixe ou mobile).

→ **Si la situation est compliquée,** difficile : appeler le **3018**. Ouvert 7j/7 jusqu'à 23h, service gratuit et confidentiel d'aide immédiate pour les jeunes, les parents et les enseignants.

→ **Dans tous les cas :** porter plainte auprès du commissariat, de la gendarmerie ou du procureur de la République.

→ **Ensuite,** la CNIL pourra vous aider à faire effacer des photos ou vidéos mises en ligne sans votre consentement ou celui de vos enfants mineurs.

LES CONSEILS

Les victimes peuvent éprouver des difficultés à raconter ce qu'elles vivent : cela peut prendre du temps. Autant de semaines, de mois pendant lesquels aucune mesure ne peut les protéger.

Les auteurs de harcèlement se nourrissent des données personnelles de leurs victimes : prénom, nom, visage, voix, adresse, entourage, liste d'amis... Il peut s'agir d'éléments (photos, vidéos) que l'ado a lui-même transmis, en toute confiance et qui sont détournés dans un esprit malveillant. Ces informations sur lesquelles se fonde le harcèlement peuvent aussi avoir été volées ou prises à l'insu de la victime ou transmises par d'anciens amis.

Gardons le lien avec nos ados, en discutant et en les incitant à s'exprimer si quelque chose ne va pas sur Internet, les réseaux sociaux, ou dans les rapports avec les autres. L'une des difficultés est de faire comprendre que le monde numérique est bien réel : il est possible de mettre en garde contre les sollicitations des inconnus, les demandes de rendez-vous ou les envois de photos, par exemple. Dans les discussions que vous avez avec votre ado, gardons en tête qu'il peut être l'initiateur ou le témoin, voire supporteur, de ces agissements. Et nous pouvons tous nous rappeler **qu'il n'est pas normal de s'habituer à la violence.**

Pour se mettre d'accord sur les règles à respecter, découvrez « Notre pacte famille » du livret *Tous en mission*.

cnil.fr/fr/gardiens-et-gardiennes-du-numerique-tous-en-mission

LES RESSOURCES

cnil.fr/fr/cyberviolences-et-cyberharcelement-que-faire

Association E-enfance :

e-enfance.org/nos-interventions/ressources/

NOTA BENE

1 - Au titre de leur obligation propre d'éducation et de surveillance de leurs enfants, les parents ont une responsabilité civile sur les actes de leurs enfants. (Arrêt de la cour de cassation 13 décembre 2022 00-13.787)

2 - Ici sont précisées toutes les sanctions « Les sanctions encourues par les auteurs de violences en ligne"
cnil.fr/fr/cyberviolences-et-cyberharcelement-que-faire

SERVICES EN LIGNE : COMPRENDRE LES ENJEUX

La définition

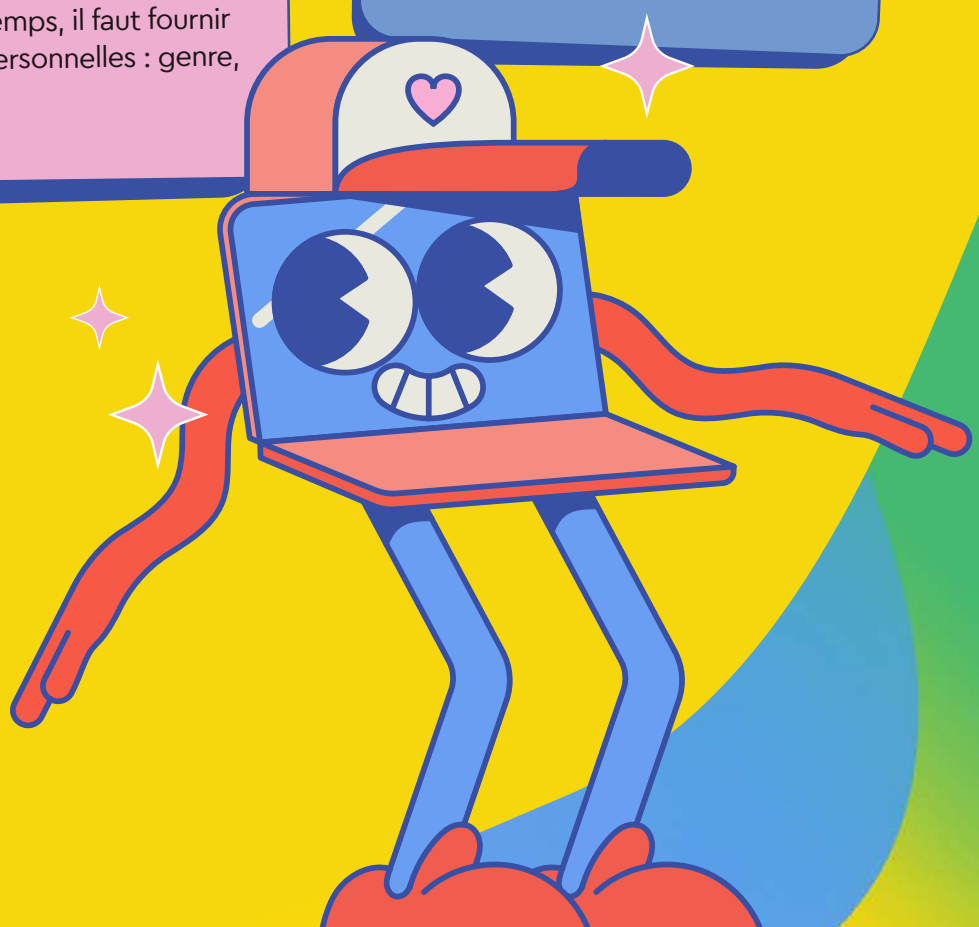
→ Jeux, musique, films, messages textes, appels vidéo... **les services en ligne sont innombrables et nous permettent chaque jour d'être en lien** avec nos amis, notre famille, de partager, d'accéder à la culture et à une multitude d'informations passionnantes.

Accessibles en quelques clics, les services en ligne nous permettent beaucoup et peuvent avoir des répercussions positives dans nos vies physiques.

Pour profiter de tous ces services, la plupart du temps, il faut fournir ses données personnelles : genre, âge, localité...

Sur nos traces

→ Pour nous proposer toujours plus d'options susceptibles de nous intéresser, les fournisseurs de service en ligne **voudraient connaître ou prédire ce que nous aimons et ce que nous n'aimons pas,** avec qui nous interagissons ou pas (encore). Nous sommes fortement susceptibles d'aimer les mêmes choses que les personnes avec lesquelles nous échangeons des messages ou que nous suivons, voire les personnes qui ont les mêmes goûts que nous mais avec lesquelles nous ne sommes pas encore en relation.



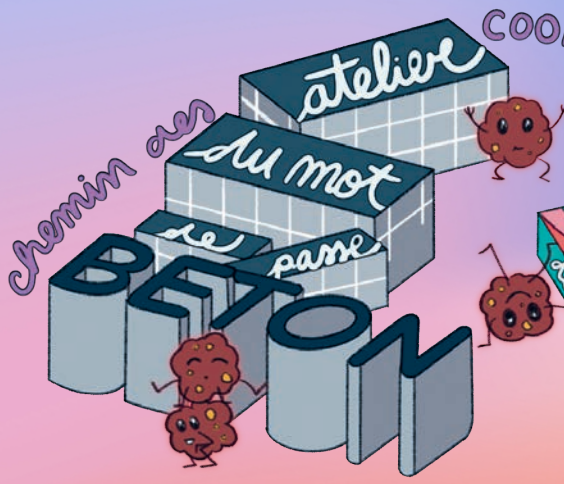
NOS VIES DANS LES ALGORITHMES

Les algorithmes* sont fabriqués sur ce principe de recommandation. **Ils analysent nos recherches, lectures, commentaires, liens avec des personnes…**
Couplés aux données personnelles que nous fournissons, ils façonnent, au fil de nos clics, un portrait de nous. Ils nous attribuent une forme de personnalité selon une liste de traits de caractères préétablie.
Ce portrait de nous est subjectif : il est bâti sur ce que l'outil pense que nous sommes, grâce à des critères liés à ce que les fournisseurs de service en ligne peuvent nous proposer et sur des listes ne pouvant, par définition, pas énumérer toutes les facettes possibles de l'humain. De ce portrait découle ce qui est nous est montré et proposé. Cela peut influencer nos choix, nos pensées, nos opinions dans nos vies « tangibles ».

La définition

***Un algorithme** est la description d'une suite d'étapes permettant d'obtenir un résultat à partir d'éléments fournis en entrée. Par exemple, une recette de cuisine est un algorithme permettant d'obtenir un plat à partir de ses ingrédients ! Dans le monde de plus en plus numérique dans lequel nous vivons, les algorithmes mathématiques permettent de combiner les informations les plus diverses pour produire une grande variété de résultats : simuler l'évolution de la propagation de la grippe en hiver, recommander des livres à des clients sur la base des choix déjà effectués par d'autres clients, comparer des images numériques de visages ou d'empreintes digitales, etc.

cnil.fr/fr/definition/algorithme



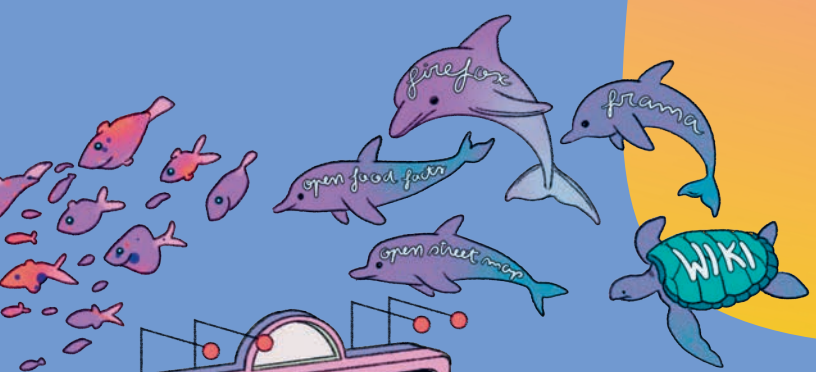
À FAIRE

- **Jeter un œil aux CGU, et politique de gestion des données personnelles, parfois nommée « confidentialité » :**
  - → Qui est l'éditeur de ce site / cette application et où est-il situé ? *(exercer ses droits n'est pas pareil d'un pays à l'autre)*
  - → À quoi servent mes données ? Combien de temps sont-elles gardées ?
  - → Sont-elles transmises ? À qui ? Pour quoi faire ?
  - → Comment puis-je exercer mes droits ?
- **Rester alerte sur ce portrait qui est fait de nous** pour éviter que les algorithmes ne nous proposent que des résultats correspondant uniquement aux goûts qu'ils ont retenus de nos usages, car cela nous enferme dans une case et limite la variété des informations auxquelles nous accédons.
  - → Certaines applications permettent de connaître le portrait qui est fait de nous.
- **Les droits liés à l'utilisation de nos données personnelles :**
  - → Être informé(e) : savoir ce qui va être fait de nos données.
  - → S'opposer : ne pas être d'accord pour que nos données soient exploitées.
  - → Accéder à ses données : savoir ce que l'on sait de nous.
  - → Rectifier ses données.
  - → Effacer ses données.
  - → Être déréférencé(e) : dans un moteur de recherche, supprimer des informations nous concernant.
  - → Emporter ses données avec soi.

CONSEILS PRATIQUES

POUR LES RÉSEAUX SOCIAUX ET AUTRES COMPTES QUE L'ON FAIT EN LIGNE (MUSIQUE, FILMS...)

- Fabriquer des mots de passe solides pour chaque service en ligne utilisé ET les garder strictement pour soi.
- Construire un pseudo ne révélant aucune information sur notre identité : ni nom, prénom, département...
- Utiliser une photo non identifiante (qui ne permet pas de nous reconnaître), un avatar.
- Mettre son compte en privé pour maîtriser son audience.
- Désactiver la géolocalisation par défaut.
- Quand on publie, éviter de donner des indications sur sa géolocalisation, son domicile, des photos de ses enfants...



CYBERSÉCURITÉ

Nos données personnelles sont très précieuses ! C'est la raison pour laquelle elles attirent tant de convoitises.

1 Des mots de passe en or massif, sinon rien !

Les mots de passe permettent un accès direct vers nos informations personnelles, autant les blinder !

→ Créer des mots de passe solides et différents pour chaque service en ligne
cnil.fr/fr/generer-un-mot-de-passe-solide

→ Utiliser un gestionnaire de mots de passe sécurisé
cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires

2 On le sait mais on ne le fait pas, **sauvegarder ses données régulièrement et à deux endroits différents,** c'est se prémunir de toute perte liée à un accident intentionnel ou non.

3 Mettre à jour les logiciels et applications dès que c'est possible

→ Des failles de sécurité peuvent se glisser dans les logiciels. Les mises à jour permettent de les corriger. Une faille de sécurité, c'est la porte ouverte à un pirate.

4 En dire publiquement le moins possible sur soi

→ Toute information personnelle à disposition de tous peut être utilisée contre nous, même quand on pense qu'on n'a rien à cacher : géolocalisation, photos...

→ Vérifier les paramètres de confidentialité de ses comptes : qui peut avoir accès à nos posts ?

5 Les wifi publics sont rarement sécurisés...

→ Pour les opérations type virement ou connexion à sa messagerie principale, il vaut mieux utiliser son forfait téléphonique (4G ou 5G).

6 Les appareils partagés c'est super, il faut juste bien **penser à se déconnecter si on s'identifie sur un site depuis un ordinateur en libre-service** (médiathèque, bibliothèque, hôtel, etc.)

7 « Bravo, vous avez gagné un téléphone ! Plus qu'1h pour le récupérer ! » : **les messages dont la provenance n'est pas familière, ou incitant à agir immédiatement méritent calme et discernement.**

L'hameçonnage ou phishing, ce sont des messages (courriels, SMS, réseaux sociaux) ou appels d'escrocs qui cherchent à nous faire paniquer et se font passer pour un organisme familier (banque, administration). Tout cela pour voler nos données personnelles ou nous escroquer.

8 Les objets connectés méritent aussi notre attention : changer les mots de passe initiaux et mettre à jour leurs logiciels, c'est bien !

9 C'est tentant mais pas forcément une bonne idée : **les contenus piratés ou non officiels peuvent contenir des virus.**

→ Installer uniquement des applications depuis les sites ou magasins officiels des éditeurs.


APPRENDRE À NAVIGUER EN PRIVÉ
PORT DE L'ARNAQUE EN LIGNE
BATEAU DES PLATEFORMES D'INFORMATION
filet des données personnelles
banc de données

NOS CONSEILS

SPÉCIAL PARENTS

1 **Garder le lien avec vos enfants, toujours et coûte que coûte,** pour rester les adultes de confiance s'ils ont des questions ou vivent des mésaventures liées à leurs activités en ligne, même si vous avez l'impression de ne pas avoir les codes ou d'être dépassé(e). Il est possible d'avoir accès à des contenus choquants sans les avoir sollicités. Les enfants doivent avoir un adulte de confiance auprès duquel ils peuvent partager leurs émotions.

2 **Se mettre d'accord ensemble sur les règles d'utilisation à la maison et en dehors.** Les règles se renégocient au fur et à mesure que les ados grandissent.

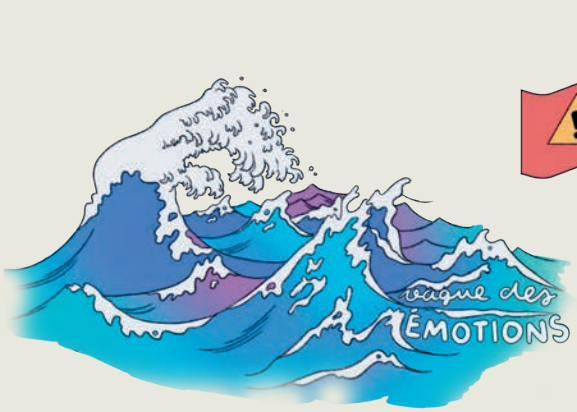
3 **Accompagner les enfants sur la protection de leur vie privée.** La vie privée, c'est ce qu'on veut garder pour soi, ne pas dire aux autres. C'est aussi ce qu'on ne veut pas que les autres révèlent sur nous. Et cela ne concerne pas seulement les autres utilisateurs, mais aussi les plateformes qui se nourrissent des informations liées à nos activités.

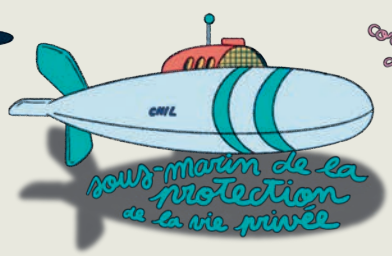
→ **Exemple de bonnes pratiques :**

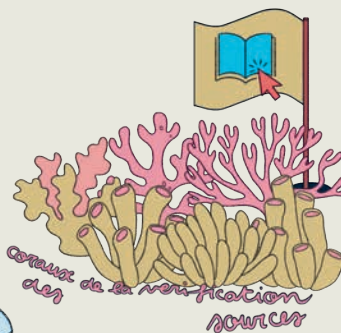
- → paramétrer son téléphone : être attentif aux réglages par défaut (géolocalisation, micro, suivi des mouvements...);
- → paramétrer les services en ligne : compte en privé, désactiver le scroll infini, utiliser un pseudonyme, un mot de passe fort, une photo de profil non identifiante, désactiver les notifications, etc.

4 **La politesse, le respect, l'humanité nous permettent à tous de bien vivre ensemble dans l'espace physique.** En ligne, c'est exactement pareil. La façon dont on s'adresse aux autres en ligne doit respecter les mêmes règles que « dans la vraie vie ». Chacun de nous fait vivre Internet et a un rôle à jouer pour en faire un espace sain. Tout ce que l'on fait et dit en ligne contribue à constituer nos identités en ligne. Pour l'instant c'est un impensé.

5 **Respecter la vie privée des enfants.** Il est bon de les accompagner sans être intrusif, sous peine de perdre leur confiance.







NOS CONSEILS

SPÉCIAL ENSEIGNANTS

Les compétences de base à acquérir par les élèves. En route vers des pratiques numériques éclairées !

1 **Maîtriser le lexique, savoir de quoi on parle quand on évoque Internet, savoir définir :** réseau Internet, réseau social, moteur de recherche, navigateur, adresse IP, cookie, algorithme, pseudonymat/anonymat, VPN, donnée personnelle, donnée personnelle sensible.

2 **L'altérité en ligne :** comprendre que l'on n'est pas seul dans l'espace numérique, même si l'on ne voit pas l'autre, contrairement à l'espace physique. La relation dans l'espace physique peut se prolonger dans l'espace numérique et les règles de vivre ensemble s'appliquent dans les deux espaces.

3 **Intégrer l'esprit scientifique en lien avec le numérique :** se poser des questions sur les systèmes numériques (notion de traçage, intérêts poursuivis, économie de l'attention, bulles de filtres), émettre des hypothèses, chercher les réponses, répondre aux questions que l'on se pose avec des sources variées et vérifiées.

4 **Réfléchir à son identité en ligne, comprendre que l'on peut être la cible de messages commerciaux et politiques.** Se poser la question des messages que l'on reçoit en ligne non pas des pairs mais des organismes tiers : pourquoi m'envoient-ils ce type de message, comment m'ont-ils identifié(e), qui sont-ils, qu'attendent-ils de moi (réaction, émotion), qu'est-ce que l'interaction avec eux peut avoir comme conséquence sur mon identité en ligne ou hors ligne ?

5 **Savoir pourquoi et comment protéger sa vie privée en ligne :** avoir des notions au sujet du profilage et de la surveillance, connaître la notion d'identité en ligne, et d'identification par des organismes tiers. Se demander l'intérêt de cette identification et se poser la question de qui sont ces organismes tiers.

6 **Savoir décoder les messages reçus personnellement ou apparus sur un fil de navigation :** comprendre la puissance de l'intelligence artificielle et l'impact sur les messages que l'on peut recevoir individuellement et à l'échelle d'un groupe, voire de la société.

7 **Savoir qu'on a des droits et qu'on peut les exercer**, savoir que la CNIL existe, ce qu'elle défend et peut faire pour aider les citoyens, même mineurs, à exercer leurs droits. Connaître les recours possibles en cas de problème : 3018 et Point de contact, Cybermalveillance, Police/Gendarmerie avec notamment la plateforme Pharos.

8 **Apprendre les cyber réflexes :** avoir un mot de passe fort pour chaque service en ligne, mettre à jour ses appareils, paramétrer sa confidentialité, comprendre les différentes techniques de piratage (hameçonnage) et savoir les déjouer. Connaître et exercer les gestes à mettre en place pour naviguer en ligne tout en maintenant un niveau de sécurité acceptable (paramétrage).

NOTES

Ce numéro **CHUT! EXPLORE** est édité pour le compte de la Commission nationale de l'informatique et des libertés (CNIL) par Chut! Explore, association N° RNA W751270150. **Illustrations :** Adeline Schöne. **Crédits :** CNIL.
CONTACT explore@chut.media / educnum@cnil.fr **ISSN** 3003-1346 **CPPAP :** 0125 G 95235 **PARUTION** Bimestriel avec Supplément.
Dépôt légal à parution.

CHUT!EXPLORE
EXPLORATIONS NUMÉRIQUES

Chut! Explore est le magazine de culture numérique pour enfants et adolescents. Nous avons pour mission de promouvoir la culture et l'éducation au numérique auprès des jeunes, afin de leur permettre de maîtriser ces outils, en saisir les enjeux et les risques, et se préparer aux métiers de demain.

CNIL
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

La CNIL est la Commission nationale de l'informatique et des libertés. Nous avons pour mission de protéger vos données personnelles et de faire respecter votre vie privée. Nous aidons également les personnes à connaître et comprendre leurs droits pour mieux maîtriser leurs données personnelles.