

**TERRITOIRE  
NUMÉRIQUE  
ÉDUCATIF**  
Corse du Sud



**" Éducation numérique  
et données personnelles "**

par Mme Jennifer Elbaz

Chargée de mission éducation au numérique  
CNIL Commission nationale de l'informatique et des libertés

# Sommaire

- Une minute, une question
- Mais que fait la CNIL ?
- Les données personnelles, ça nous concerne ?
- Protéger les données personnelles, mais pourquoi ?
- Comment faire ?
- Qui a les droits ?
- Ressources à disposition
- Travaux en cours



**TERRITOIRE  
NUMÉRIQUE  
ÉDUCATIF**  
Corse du Sud

# Une minute, une question

# Une minute, une question

**Pour vous, la vie privée, qu'est-ce que c'est ?**

**Pour les jeunes, la vie privée, qu'est-ce que c'est ?**

**Dans le cadre professionnel, la vie privée, qu'est-ce que c'est ?**



**TERRITOIRE  
NUMÉRIQUE  
ÉDUCATIF**  
Corse du Sud

# Mais que fait la CNIL ?

## Ça veut dire quoi « CNIL » ?

**A** Cercle neuronal  
des idées libérées.

**B** Centre naturel des iguanes  
du Languedoc.

**C** Commission nationale  
de l'informatique et des libertés.



! La Commission nationale  
de l'informatique et  
des libertés (CNIL) est une  
administration de l'État.  
Une de ses missions :  
aider les personnes à faire  
effacer des images ou  
des renseignements  
qui sont en ligne et qui les  
concernent.

# Point de départ

Le Monde

ACTUALITÉS ▾

ÉCONOMIE ▾

VIDÉOS ▾

DÉBATS ▾

CULTURE ▾

LE GOÛT DU MONDE ▾

SERVICES ▾

ARCHIVES

## Une division de l'informatique est créée à la chancellerie " Safari " ou la chasse aux Français

En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le Journal officiel va publier un arrêté créant une " division de l'informatique " au ministère de la justice, celui de l'intérieur met la dernière main à la mise en route d'un ordinateur puissant destiné à rassembler la masse énorme des renseignements grappillés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à définir chaque Français par un " identifiant ", qui ne définit que lui, maintenant terminé, est l'objet de convoitises ardentes; le ministère de l'intérieur y souhaite jouer le premier rôle. En effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, une puissance sans égale. Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebattu : celui des rapports des libertés publiques et de l'informatique. Son importance exigerait qu'il en fût, au Parlement, publiquement débattu. Tel ne paraît pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministère de la justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

Par PHILIPPE BOUCHER.

# Loi Informatique & Libertés 6 janvier 1978

## Article 1er

« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »

<https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article1>



## 4 missions

- Informer et protéger les droits
- Accompagner la conformité, conseiller
- Anticiper et innover
- Contrôler et sanctionner



**TERRITOIRE  
NUMÉRIQUE  
ÉDUCATIF**  
Corse du Sud

# Les données personnelles, ça nous concerne ?

# Une donnée personnelle, concrètement...

**C'est une information permettant d'identifier ou de caractériser une personne identifiée ou identifiable**

Nom, prénom

Voix

Visage

Numéro de téléphone...

# Une donnée personnelle sensible

**Ces données ont un statut particulier, elles sont protégées**

Religion

Opinion politique

Appartenance syndicale

Orientation sexuelle

Etat de santé

# Une donnée biométrique

**Est légalement considérée comme sensible**

Iris de l'œil  
Empreinte digitale  
ADN

# Parcours de vie de nos données personnelles

## **Nous renseignons nous-mêmes les organismes**

Quand on crée un compte en ligne ou dans un magasin par exemple

## **De nos gestes, traces, en ligne ou hors ligne, nos données sont analysées et soumises à interprétation**

En sont déduits nos goûts, nos opinions...



—  
**TERRITOIRE  
NUMÉRIQUE  
ÉDUCATIF**  
Corse du Sud



# Protéger les données personnelles, mais pourquoi ?

# La dure vie des données personnelles

## Les attaques

Incident de sécurité d'origine malveillante ou non, se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

- Violation de données
- Rançongiciel
- Credential Stuffing



# Côté professionnel

## Dès la collecte, penser à la suppression

- Collecter
- Enregistrer
- Organiser
- Conserver
- Modifier
- Combiner
- Transmettre
- Stocker

= traiter des données



---

**TERRITOIRE  
NUMÉRIQUE  
ÉDUCATIF**  
Corse du Sud

# Comment faire ?

# Geste gratuit et simple N°1 : le mot de passe

## Fort et différent pour chaque service en ligne

Sur notre site, un générateur de mots de passe

Saisir votre phrase

Saisir une phrase, de préférence ponctuée

**Pour un mot de passe de douze caractères ou plus, votre phrase doit contenir au moins :**

- 1** Un **nombre**
- 2** Une **majuscule**
- 3** Un **signe de ponctuation** ou un **caractère spécial** (dollar, dièse, ...)
- 4** Une **douzaine de mots**

<https://www.cnil.fr/fr/generer-un-mot-de-passe-solide>

Pour aller plus loin : [https://www.cnil.fr/sites/default/files/atoms/files/recommandation-mots-de-passe\\_annexe2\\_tableau-correspondance.pdf](https://www.cnil.fr/sites/default/files/atoms/files/recommandation-mots-de-passe_annexe2_tableau-correspondance.pdf)

Conseil CNIL pour gérer les mots de passe : utiliser un gestionnaire de mots de passe : KEEPASS

# Geste gratuit et simple N°2 : chiffrer les données

Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement.

Le chiffrement est une méthode qui consiste à protéger ses documents en les rendant illisibles par toute personne n'ayant pas accès à une clé dite de déchiffrement.

Sur le site de la Cnil vous trouverez un tuto pour chiffrer vos données

## Technique n° 2 : abriter un ou plusieurs documents dans un répertoire chiffré

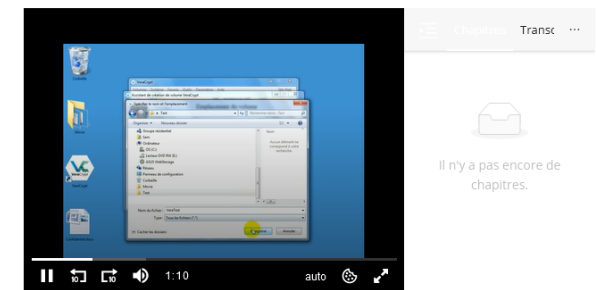
Plutôt que chiffrer les documents un par un, il est possible de créer des partitions chiffrées. Une partition chiffrée est une sorte de répertoire chiffré qui, une fois ouvert, se présentera comme un disque réseau supplémentaire.

Différents logiciels fournissent cette fonctionnalité, comme, par exemple, Zed! de Prim'X Technologies, Bitlocker de Microsoft ou encore Veracrypt. Ce dernier étant un logiciel libre et gratuit, c'est celui-ci que nous avons choisi pour notre tutoriel.

### TUTORIEL : UTILISER VERACRYPT

Ce tutoriel vous montre comment chiffrer un espace de travail sur votre PC en tout simplicité. Il s'adresse aux internautes qui souhaitent s'initier au chiffrement à des fins personnelles ou dans le cadre de leur travail.

<https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires>



# Geste simple N°3 : sauvegarder régulièrement

Problème technique : éviter des pertes de données lors des manipulations de dossiers

Erreur humaine : suppressions par inadvertance

Indisponibilité des données : se prémunir des attaques par rançongiciel

# Mémo pro

## 1. Protéger l'accès aux données papier ou numériques

Sécuriser pour maîtriser les accès numériques  
Protéger l'accès aux dossiers papier (sous clé ?)

## 2. Se poser la question des données collectées

Quelles données personnelles dois-je absolument fournir pour accéder au service ?

## 3. Accès aux données

Qui a accès aux données ?  
Pour combien de temps ?  
Où sont stockées les données ?

## 4. Exercer les droits numériques

Ergonomie des plateformes : information adaptée ?  
Chemin interne pour que les demandes soient traitées: balisé ou embouteillé ?

## 5. Responsabilité légale

Chaque personne ayant un accès aux données est responsable à son niveau



---

**TERRITOIRE  
NUMÉRIQUE  
ÉDUCATIF**  
Corse du Sud

# Qui a les droits ?

# Dès la naissance, les mêmes droits pour tous !

- Être informé
- S'opposer
- Vérifier ses données
- Rectifier ses données
- Déréférencer un contenu
- Effacer un contenu
- Emporter ses données
- Demander une intervention humaine

**Plus de droits pour vos données !**

- 1 Des données à emporter !**  
Je peux récupérer les données que j'ai communiquées à une plate-forme et les transmettre à une autre (réseau social, fournisseur d'accès à Internet, site de streaming, etc.)  

- 2 Plus de transparence**  
Je bénéficie de plus de lisibilité sur ce qui est fait de mes données et j'exerce mes droits plus facilement (droit d'accès, droit de rectification).  

- 3 Protection des mineurs**  
Les services en ligne doivent obtenir le consentement des parents des mineurs de moins de 15 ans avant leur inscription.  

- 4 Guichet unique**  
En cas de problème, je m'adresse à l'autorité de protection des données de mon pays, quelque soit le lieu d'implantation de l'entreprise qui traite mes données.  

- 5 Sanction renforcée**  
En cas de violation de mes droits, l'entreprise responsable encoure une sanction pouvant s'élever à 4% de son chiffre d'affaires mondial.  

- 6 Consécration du droit à l'oubli**  
Je peux demander à ce qu'un lien soit déréférencé d'un moteur de recherche ou qu'une information soit supprimée s'ils portent atteinte à ma vie privée.  


Nouveau Règlement européen sur la protection des données personnelles  
Avec le quatre-vingt-neufième article, l'article 84 du règlement sur la protection des données personnelles, les entreprises ont le droit de s'adapter aux nouvelles règles de données. Les entreprises ont le droit de choisir les données à collecter et de contrôler sur quels données personnelles. Il s'agit des données personnelles de personnes et leur offre un cadre juridique strict. Il est applicable depuis le 25 mai 2018 dans toute l'UE.

**CNIL**  
Commission nationale  
informatique et libertés

[https://www.cnil.fr/sites/default/files/atoms/files/affiche-plus\\_de\\_droits.pdf](https://www.cnil.fr/sites/default/files/atoms/files/affiche-plus_de_droits.pdf)



# Exercice des droits

## 1. Trouver le responsable de traitement

Politique de confidentialité

CGU

Mentions légales

## 2. Contacter le responsable de traitement

Et garder tous les écrits

## 3. Pas de nouvelles au bout d'un mois ?

Porter plainte auprès de la CNIL





**TERRITOIRE  
NUMÉRIQUE  
ÉDUCATIF**  
Corse du Sud

# Ressources à disposition

# Campagne 8-10 ans

## Un bouquet de ressources pour comprendre, et apprendre

- 4 vidéos
- Poster/glossaire
- Quiz
- Jeu de cartes
- Diplôme
- Livret enseignants
- Livret parents



<https://www.cnil.fr/fr/prudence-sur-internet-les-nouvelles-ressources-pedagogiques-de-la-cnil-pour-les-8-10-ans>

# Vidéos

Influenceur Kevin Tran



PROTÉGER SA VIE PRIVÉE ! - LE RIRE JAUNE



Kevin Tran 陈科... ✓  
5,52 M d'abonnés

S'abonner

👍 352 k



➦ Partager



# Vidéos

## PIX

- Connaître les recommandations pour le choix d'un mot de passe robuste.
- Identifier des situations d'arnaque par manipulation psychologique (hameçonnage, usurpation d'identité, faux support informatique).
- Connaître les notions de données à caractère personnel, de recoupement et d'anonymisation
- Connaître et utiliser la capacité du GPS et d'une adresse IP à géolocaliser un appareil.
- Maîtriser l'accès à ses données lors de l'installation d'une application.
- Reconnaître des situations de cyberharcèlement et savoir comment réagir.

<https://pix.fr/actualites/sensibilisation-au-numerique-pix-participe-a-la-prevention-pour-les-eleves-de-6e>

# Jeu immersif

6 missions :

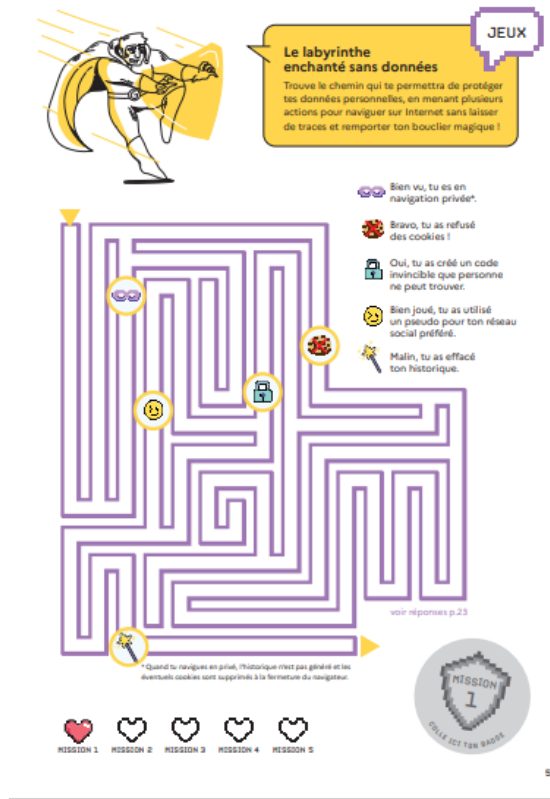
- Jeux vidéo
- Vie privée
- Infox
- Cyberharcèlement
- Economie de la donnée
- Mécanismes de l'influence





# Livret lié au jeu immersif

## Côté jeunes



<https://www.cnil.fr/fr/gardiens-et-gardiennes-du-numerique-tous-en-mission>

# Livret lié au jeu immersif

## Côté adultes



**MISSION 2**

## Reconnaître les infox

**C'est quoi une "infox" ?**

Une "fake news", ou "infox" en français, désigne une information mensongère pour induire une personne en erreur. La propagation d'une infox est facilitée par la rapidité de diffusion et l'effet d'amplification des réseaux sociaux, des messages instantanés...

**Est-ce que c'est grave ?**

Les infox peuvent propager de la désinformation sur des sujets cruciaux tels que la santé, la politique et la science, ce qui peut avoir des conséquences néfastes allant de la confusion du public à la manipulation des opinions et des comportements. En alimentant les divisions sociales et en exacerbant les tensions, les infox peuvent contribuer à polariser les débats et mettre en danger la démocratie.

**Comment les repérer ?**

Pour lutter contre les risques d'infox, il est essentiel de développer des compétences en pensée critique et en vérification des faits, afin de contrer les effets nocifs des infox et préserver l'intégrité de l'information. Doter les enfants (et les adultes !) d'outils nécessaires au développement de la pensée critique, leur permet de devenir des lecteurs et lectrices avisés et responsables de l'information. Il est crucial d'**apprendre à questionner les contenus, apprendre à observer les sources d'information, à vérifier les faits et à rechercher des avis différents.** Aider les enfants à identifier les signes caractéristiques de contenus douteux (titres sensationnalistes, images manipulées...) permet d'aller dans ce sens.

**Plus de 40%** des utilisateurs de TikTok ont confiance dans le contenu des influenceurs s'ils ont beaucoup d'abonnés.

Source : IJOP, Fondation Jean Jaurès, Reboot, 2022

**À FAIRE**

**64%** des jeunes entre 18 et 24 ans utilisent Internet comme source principale d'information.

Source : "Observation Reboot de l'information et du raisonnement critique - volet 2 : l'attention journalistique et les pratiques des Français en matière d'information et de raisonnement critique" IJOP, 19 avril 2022

**Pour les parents**

**À LA MAISON**  
Familiarisez-vous avec le décodage des fausses informations et éduquez vos enfants à l'esprit critique.

- LA VIDÉO : C'est quoi les infox ?
- LE POSTER : Info ou Infox, les 11 pièges à éviter
- LE KIT DECODER : Pour dénicher les fausses informations

**Pour les enseignants**

**EN CLASSE**  
Organisez des sessions et des programmes ludiques à l'éducation aux médias et à l'information.

- LE LIVRET PÉDAGOGIQUE : Les essentiels d'éducation aux médias et à l'information
- LE PROGRAMME ÉDUCATIF : Éducation aux médias et à l'information
- LE LIVRET : Info ou Infox, ne tombez pas dans le panneau !



# Livret lié au jeu immersif

## Pacte en famille

NOTRE  
PACTE  
FAMILLE

Complétez en famille, de façon  
égaleitaire, votre pacte pour garantir et  
favoriser l'implication de chacun. Vive  
l'utilisation positive, responsable et  
sécurisée du numérique !

Sécurité

Protéger nos vies numériques

Ensemble, nous nous engageons à fournir un environnement en ligne sûr à l'aide de filtres et de contrôles parentaux.

Les « enfants gardiens » s'engagent à ne jamais dévoiler leur nom, adresse et autres précieuses informations personnelles, à moins que les « parents gardiens » ne donnent leur feu vert, et à ne pas s'inscrire sur les sites qui ne sont pas de leur âge.

Les « parents gardiens » aideront à choisir des contenus en ligne appropriés à l'âge des enfants.

COCHEZ

Respect

Agir en sagesse

Les « parents gardiens » s'engagent à créer un espace de dialogue non jugeant et bienveillant sur l'usage du numérique avec leurs enfants.

Les « enfants gardiens » s'engagent à toujours utiliser des commentaires et actions respectueuses, bienveillantes, positives et à demander l'avis de leurs parents avant de s'inscrire sur les plateformes en ligne.

COCHEZ

Dialogue

Parler et écouter

Les « enfants gardiens » s'engagent à ne jamais garder le silence s'ils rencontrent des difficultés et à partager leurs expériences numériques.

Les « parents gardiens » s'engagent à écouter dans le respect, sans jugement, et à apporter leur aide et soutien en cas de besoin.

Ensemble, nous nous engageons à discuter pour faire évoluer les règles s'il en est nécessaire.

COCHEZ

Équilibre

Équilibrer les mondes réel et virtuel

Chaque membre de la famille s'engage à limiter son temps d'écran

L'ensemble des membres de la famille s'engage à déconnecter les écrans pendant les moments de repas.

Les « enfants gardiens » s'engagent à répondre à l'appel des « parents gardiens » pour les rejoindre à faire une activité hors écran.

COCHEZ

Nos règles bonus

.....

.....

.....

.....

.....

.....

COCHEZ

Engagements

Nos engagements

**TEMPS D'ÉCRAN PAR JOUR LA SEMAINE**

..... heures/jour maximum

**LE WEEK-END**

..... heures/jour maximum

**TEMPS ÉCRAN / HORS ÉCRAN**

pas avant ..... h

pas après ..... h

**MOMENTS SANS ÉCRAN**  
coloriez les moments sans écran

A table   
  en vacances   
  avec des amis

**JOURS SANS ÉCRAN**  
coloriez les jours sans écran

Signatures

« PARENTS GARDIENS » :

.....

« ENFANTS GARDIENS » :

.....

Date : .....

# Les posters

## 10 conseils pour rester net sur le web



**10 conseils de la CNIL pour rester Net sur le Web**

- 1 Réfléchir avant de publier**  
Sur internet, tout le monde peut voir ce que tu publies : photos, vidéos, opinions, etc.
- 2 Respecter les autres**  
Tu es responsable de ce que tu publies sur les réseaux sociaux... Ne fais pas aux autres ce que tu ne voudrais pas que ton fils fasse.
- 3 Ne pas tout dire**  
Donner le maximum d'informations sur soi en ligne, c'est se protéger ! Mieux vaut ne pas communiquer les opinions, la religion ou ton numéro de téléphone...
- 4 Sécuriser ses comptes**  
En paramétrant les profils sur les réseaux sociaux, tu restes maître des informations que tu souhaites partager.
- 5 Créer plusieurs adresses mail**  
Tu peux par exemple utiliser une adresse pour les jeux vidéo, une pour les amis et une autre boîte e-mail pour les réseaux sociaux.
- 6 Faire attention à tes photos et tes vidéos**  
Envoyer, publier une photo ou une vidéo garantit de soi ou des autres, c'est rendre une diffusion incontrôlable.
- 7 Utiliser un pseudonyme**  
Seules les personnes à qui tu l'auras communiqué sauront qu'il s'agit de toi et sauront tes aventures sur le net.
- 8 Protéger ses mots de passe**  
Il faut qu'il soit difficile à deviner et différent pour chaque service. Évite d'utiliser les numéros ou bien la date de naissance par exemple. Et surtout, garde-le pour toi !
- 9 Nettoyer ses historiques**  
Pour éviter d'être tracé, il est conseillé d'effacer régulièrement les historiques de navigation et d'utiliser la navigation privée si tu utilises un ordinateur ou un smartphone qui n'est pas le tien.
- 10 Surveiller sa réputation en ligne**  
Taper ton nom dans un moteur de recherche te permet de savoir ce qui est dit sur toi sur internet et quelles informations circulent.

Partage ces conseils avec tes amis et ta famille pour qu'ils protègent eux aussi leur vie privée !

**CNIL**  
COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉS

Retrouvez d'autres conseils sur [www.cnil.fr](http://www.cnil.fr)

[https://www.cnil.fr/sites/default/files/atoms/files/poster\\_10-conseils-pour-rester-net-sur-le-web\\_ok.pdf](https://www.cnil.fr/sites/default/files/atoms/files/poster_10-conseils-pour-rester-net-sur-le-web_ok.pdf)

## 5 conseils pour se protéger sur les réseaux sociaux



**5 CONSEILS POUR PROTÉGER ma vie privée sur les réseaux sociaux**

- 1 J'AI CONSCIENCE**  
que mes données personnelles ont de la valeur ! Toutes les informations que je poste sur YouTube et Instagram sont réutilisées. Pour savoir comment sont exploitées mes données de géolocalisation, mes photos, mes habitudes, mes like, je consulte les Conditions Générales d'Utilisation.
- 2 JE PROTÈGE**  
ma vie privée en utilisant des pseudonymes et des avatars selon les services que j'utilise et en fonction de mes usages. Je veille à bien distinguer mes amis de mes simples connaissances... en m'assurant de leur identité.
- 3 JE VERRONILLE**  
mon compte ! D'abord en le sécurisant avec un mot de passe fort et en activant les options complémentaires comme la « double authentification ». Ensuite en réglant mes paramètres de confidentialité pour limiter l'accès à mon profil ou à mes publications à des utilisateurs que j'ai choisis.
- 4 J'ANTICIPE**  
les conséquences de mes publications ! Internet est un lieu public où je peux laisser des traces, même sur Snapchat ! Avant de publier, je m'assure que mes publications ne nuisent ni à ma réputation, ni aux autres, ni à moi.
- 5 JE VÉRIFIE**  
les informations auxquelles j'ai accès avant de les partager ou de cliquer dessus. Dernière certaines publications virales se cachent une « fake news », une arnaque, un contenu qui peuvent nuire à une personne... et parfois un programme malveillant.

Mette d'utiliser toujours les mêmes réseaux sociaux ? Consultez la cartographie des outils éditoriaux qui protègent mieux votre vie privée.

**CNIL**  
COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉS

[https://www.cnil.fr/sites/default/files/atoms/files/affiche\\_gn-cnil\\_5\\_conseils\\_pour\\_protéger\\_sa\\_vie\\_privée.pdf](https://www.cnil.fr/sites/default/files/atoms/files/affiche_gn-cnil_5_conseils_pour_protéger_sa_vie_privée.pdf)

# Poster Cyber Réflexes

## CYBER RÉFLEXES

### Se protéger sur Internet

#### 1 DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE COMPTE TU CHOISIRAS

Un mot de passe c'est comme une clé propre à chaque porte, elle te protège de l'intrusion. Si tu te fais voler un mot de passe que tu utilises pour différents sites web ou applications, ils pourront tous être piratés !

**BONNES PRATIQUES**

- Utiliser des mots de passe suffisamment longs, complexes et surtout différents pour chaque compte.
- Les garder secrets et privilégier un gestionnaire de mots de passe sécurisé pour les conserver.

#### 2 LES MISES À JOUR DE TES APPAREILS SANS TARDER TU FERAS

Les failles de sécurité de tes logiciels, applications et matériels sont comme des portes laissées ouvertes pour les pirates. Ils peuvent les utiliser pour accéder à tes données personnelles ou les voler.

**BONNES PRATIQUES**

- Faire les mises à jour des logiciels, applications et appareils, dès qu'elles te sont proposées pour corriger leurs failles de sécurité.
- Activer les options de mises à jour automatiques chaque fois que c'est possible.

#### 3 EN LIGNE, LE MOINS POSSIBLE SUR TON IDENTITÉ TU DIRAS

Publier et partager tes données personnelles sur Internet (nom, prénom, adresse mail, photos, vidéos, vocaux...) peut les exposer à une utilisation malveillante.

**BONNES PRATIQUES**

- Éviter de divulguer tes données personnelles et celles de tes connaissances.
- Vérifier les paramètres de confidentialité de tes comptes pour définir ce qui peut être visible par les autres.

#### 4 EN LIEU SÛR, UNE COPIE DE TES DONNÉES TU CONSERVERAS

Copier tes données, c'est les sauvegarder pour éviter de les perdre en cas de piratage, de vol, de panne ou de casse de tes appareils.

**BONNE PRATIQUE**

- Penser à faire régulièrement des sauvegardes de tes données sur un autre support (clé USB, disque externe, cloud...) pour pouvoir les retrouver en cas de problème.

#### 5 DES MESSAGES INATTENDUS ET ALARMANTS TOUJOURS TU TE MÉFIERAS

L'hameçonnage ou phishing, ce sont des messages (courriels, SMS, réseaux sociaux) ou appels d'escrocs qui se font passer pour un organisme familier (banque, administration...). Ces arnaques visent à te voler des informations personnelles et bancaires, te faire télécharger un virus ou directement l'escroquer.

**BONNES PRATIQUES**

- Toujours te méfier et ne pas te précipiter pour cliquer ou répondre.
- Vérifier toujours l'information par toi-même, en te connectant à ton compte sur le service concerné.

#### 6 LES CONTENUS PIRATÉS OU NON OFFICIELS TU ÉVITERAS

Des virus qui peuvent pirater tes appareils ou tes comptes sont souvent présents dans les logiciels ou jeux piratés, les extensions de triche de jeux vidéo, les sites de streaming illégaux...

**BONNES PRATIQUES**

- Ne pas télécharger des contenus illégaux ni des solutions non officielles.
- Installer uniquement des applications depuis les sites ou magasins officiels des éditeurs.



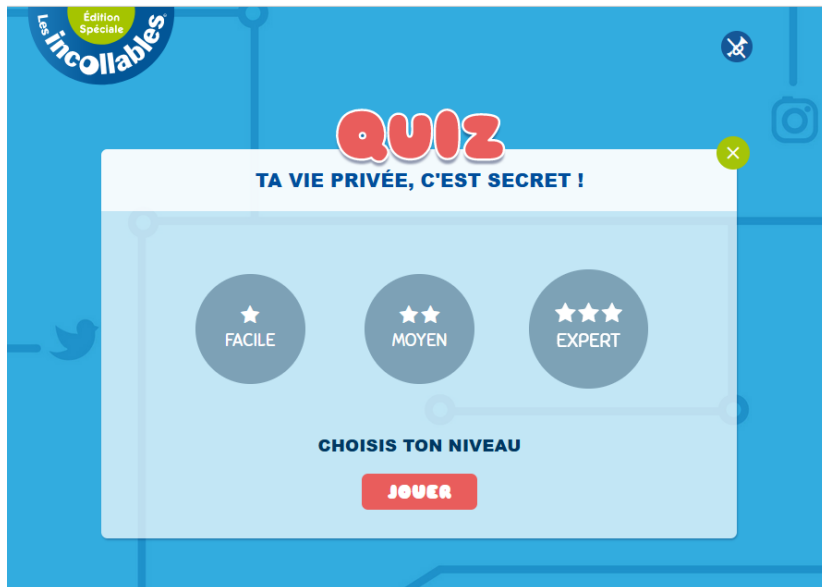



**PLUS DE CONSEILS SUR**  
**CNIL.FR**  
**CYBERMALVEILLANCE.GOUV.FR**

# Les Incollables

3 niveaux

En Français et en Anglais



<https://quiz-digital-incollables.playbac.fr/ta-vie-privee-cest-secret/30>

# Le MOOC de la CNIL

Disponible 24/7, même les jours fériés



<https://atelier-rgpd.cnil.fr/>



---

**TERRITOIRE  
NUMÉRIQUE  
ÉDUCATIF**  
Corse du Sud

# Travaux en cours

# Travaux numériques adolescent

1. Revue de littérature sur les usages numériques des adolescents,
2. Enquête qualitative auprès des adolescents,
3. Enquête quantitative auprès des parents,
4. Mise à l'épreuve du dispositif d'éducation au numérique destiné aux adolescents et à leurs prescripteurs.

# Revue de littérature scientifique

## **Les adolescents entretiennent un rapport paradoxal au numérique et à la vie privée**

- La recherche d'interaction et de reconnaissance encourage les adolescents à partager leur intimité en ligne et communiquer de façon abondante.
- Les déboires de leurs grands frères et sœurs (« génération pots cassés ») les amènent à développer leurs propres stratégies de protection de leur vie privée en ligne.

## **L'adolescence est un moment de recherche d'autonomie vis-à-vis du groupe familial voire de l'institution scolaire**

- On valorise les activités et espaces à l'abri des adultes

## **La (re)production des inégalités par le numérique**

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



# Enquête qualitative

Un apprentissage du numérique **dynamique** : entrée progressive dans le numérique, expérience numérique nourrie par **les essais-erreurs**

- Comment équiper les explorations adolescentes ?

De nombreuses **stratégies de protection de la vie privée** (publication éphémères, no face, anagrammes, etc.), avec une approche par les risques (les risques sont toujours arrimés à des dangers concrets)

- Comment concrétiser des risques abstraits ?

Une acceptabilité du contrôle parental qui **dépend du capital numérique et de la disponibilité des parents**

- Comment accompagner la diversité des profils parentaux ?

<https://linc.cnil.fr/numerique-adolescent-et-vie-privee-episode-2-au-contact-des-collegiennes-et-collegiens>

## Auteur

Jennifer ELBAZ

## Fonction

Chargée de mission éducation au numérique

## Contact

[jelbaz@cnil.fr](mailto:jelbaz@cnil.fr)