FÉDÉRATION WALLONIE-BRUXELLES | Enseignement

RECUEIL D'ACTIVITÉS

S1

Numérique

Sécurité

Réalisé par l'Administration générale de l'Enseignement
Service général du Numérique éducatif

Ce recueil d'activités aborde le champ **« Sécurité »** du volet numérique du référentiel de la Formation Manuelle, Technique, Technologique et Numérique (FMTTN). L'objectif est d'amener l'élève à gérer et à sécuriser, de manière autonome, son identité et son bien-être numériques.

À travers ces activités, l'élève développe un comportement éthique et responsable, tout en apprenant à respecter les droits numériques liés à la diffusion des données.

Le document s'articule autour de **cinq sections thématiques**. Chaque section regroupe des attendus du référentiel abordés dans les activités proposées. Chaque activité est organisée selon la structure suivante : un titre, un objectif et un déroulement.

En matière de sécurité, rien n'est jamais définitivement acquis. Face à l'émergence constante de nouvelles ruses et menaces, ce recueil se veut une **base de discussion non exhaustive et non figée**. Les supports fournis sont des leviers permettant à l'enseignant/l'enseignante de rebondir, d'apporter des réponses claires et, surtout, d'ouvrir le débat avec les élèves.

Le but essentiel de ce champ est de favoriser la prise de conscience. En discutant de situations réelles, les élèves apprennent à repérer que certains de leurs comportements numériques ont des conséquences concrètes qu'ils ne peuvent plus ignorer.

Chaque thématique est associée à un chapitre du parcours dédié sur e-classe.be/numerique-s1-securite.

Table des matières des thématiques abordées

1 Gérer son empreinte numérique
Propositions d'activités

Attendus visés

- **Compétence** : Gérer son identité numérique, ses traces, ses données personnelles, de manière responsable
- **Savoir** : Utiliser, adéquatement en contexte, les termes dont profil, protection de la vie privée
- **Savoir** : Identifier et reconnaitre les avantages de la gestion de son identité numérique en termes de préservation de ses droits et de responsabilité
- **Savoir :** Expliquer qu'il existe des collectes de données actives (profils, formulaires, messages, tags…) et passives (métadonnées, cookies, géolocalisation…)
- **Savoir-faire** : Repérer les informations relatives à la vie privée, lors de l'encodage de données personnelles, y compris avec une IA
- **Savoir-faire** : Paramétrer les options de confidentialité d'un compte
- **Savoir-faire** : Effacer toute trace de connexion sur un équipement partagé

Exemples d'activités

Enquête sur mon identité numérique

Objectifs : prendre conscience de son empreinte numérique, identifier les données personnelles (visibles et invisibles) et comprendre comment elles permettent de reconstituer un profil.

Déroulement de l'activité :

- **Création d'un profil fictif** (Support 1.1)
  Les élèves choisissent un nom, un prénom ou un pseudonyme (le leur ou un profil fictif fourni). Ils effectuent une recherche sur Internet et notent tous les résultats trouvés : sites, images, profils ou commentaires…
- **Classification de données** (Support 1.2)
  Les élèves classent ensuite les informations récoltées en deux catégories : les données publiques et les données privées.
- **Analyse de risque données sensibles** (Support 1.3)
  Les élèves identifient les informations sensibles et évaluent les risques associés à leur diffusion.
- **Identification des données** (Support 1.4)
  Les élèves analysent une publication (photo ou message) pour distinguer les données visibles et repérer les éléments d'identification, tels que l'image de profil, le pseudonyme ou les publications associées.
- **Analyse des données « invisibles »** (Support 1.5)
  L'enseignante/l'enseignant révèle ensuite les données invisibles potentielles (date, lieu, appareil, etc.) afin que les élèves puissent compléter leur analyse.

- **Enquête ou puzzle** (Supports 1.6 - 1.7)
  Sous forme d'enquête ou de puzzle, les élèves reconstituent le profil d'une personne en s'appuyant sur un ensemble de traces numériques fournies.
- **Localisation des paramètres de confidentialité** (Support 1.8)
  Les élèves observent différentes interfaces pour localiser les paramètres de confidentialité et expliquer leur utilité.
- **Synthèse des bonnes pratiques** (Support 1.9)
  Une mise en commun permet de synthétiser les bonnes pratiques pour protéger son identité numérique.

Maitriser ses données et sa présence en ligne

Objectif : comprendre la circulation des données et les enjeux de leur collecte (notamment par l'IA), afin de savoir configurer et protéger son compte de manière autonome.

Déroulement de l'activité :

- **Classification de données** (Support 2.1)
  Les élèves reçoivent une liste d'informations (photo, âge, localisation, contacts, etc.) qu'ils répartissent entre données publiques et privées. Ils justifient ensuite leurs choix en groupe, puis confrontent leurs réponses avec celles de leurs camarades.
- **Analyse des données** (Support 2.2)
  Les élèves analysent diverses situations (création de compte, publication, formulaire) pour identifier les données transmises volontairement par l'utilisateur.
- **Observation des données** (Support 2.3)
  À partir d'exemples concrets, les élèves découvrent les données collectées automatiquement, telles que les cookies ou la géolocalisation.
- **Identification des accès aux données** (Support 2.4)
  À partir d'un scénario (publication d'une photo), les élèves identifient l'ensemble des personnes ou organisations susceptibles d'y accéder.
- **Schématisation du parcours des données** (Support 2.5 - 2.6)
  Les élèves réalisent un schéma du parcours de la donnée pour visualiser son cheminement entre les différents acteurs : amis, plateformes, annonceurs ou moteurs de recherche.
- **Classification de données** (Support 2.7)
  Les élèves discutent des finalités de la collecte de données (publicité, personnalisation, entraînement des IA, etc.) et les répartissent en deux catégories : les usages utiles et les usages problématiques.
- **Paramétrage de confidentialité** (Support 2.8)
  Les élèves accèdent à un compte fictif ou à des captures d'écran pour explorer les paramètres de confidentialité. Ils modifient ensuite ces réglages afin de limiter l'accès à leurs informations personnelles.

- **Suppression de ses traces sur un appareil partagé (Support 2.9)**
  Les élèves identifient les actions nécessaires pour effacer leurs traces sur un appareil partagé, telles que la déconnexion des comptes, la suppression de l'historique et le nettoyage des cookies.

Ressources

Pour approfondir le sujet ou compléter ces activités avec des exercices, vous trouverez des ressources gratuites sur :
e-classe.be/numerique-s1-securite

Enquête sur mon identité numérique

Objectifs : prendre conscience de son empreinte numérique, identifier les données personnelles (visibles et invisibles) et comprendre comment elles permettent de reconstituer un profil.

Support 1.1 : Création d'un profil fictif

Les élèves choisissent un nom, un prénom ou un pseudonyme (le leur ou un profil fictif fourni). Ils effectuent une recherche sur Internet et notent tous les résultats trouvés : sites, images, profils ou commentaires…

Exemple concret

Nom : Lucas Martin **Pseudonyme** : Luki_2009

Résultats bruts de recherche sur un moteur de recherche

1. Profil Instagram : @Luki_2009 (photo de profil visible)
2. Photo de groupe devant une école (uniforme identifiable)
3. Commentaire sur une vidéo YouTube (« trop bien ce jeu ! »)
4. Profil TikTok avec vidéos de danse
5. Pseudo utilisé sur un forum de jeux vidéo
6. Score en ligne sur un jeu (classement public)
7. Photo d'anniversaire (gâteau + prénom visible)
8. Publication Facebook d'un parent (« Joyeux anniversaire Lucas ! 14 ans 🎂 »)
9. Vidéo filmée dans une chambre (objets personnels visibles)
10. Adresse électronique partiellement visible (luki2009@gmail…)
11. Photo avec géolocalisation activée (parc local identifiable)
12. Liste d'amis publics sur un réseau social
13. Commentaire sur un blog scolaire
14. Participation à un tournoi sportif (nom affiché sur un site)
15. Photo d'équipe sportive avec nom du club
16. Avis laissé sur une application (pseudo + ville)
17. Story montrant un trajet quotidien (école > maison)
18. Capture d'écran d'un jeu avec identifiant visible
19. Publication mentionnant « en vacances à la mer »
20. Profil sur une plateforme éducative (prénom + classe)

Proposition d'outil pour créer un profil fictif pour l'exercice : https://zeoob.com

Support 1.2 : Classification de données

Les élèves choisissent un nom, un prénom ou un pseudonyme (le leur ou un profil fictif fourni). Ils effectuent une recherche sur Internet et notent tous les résultats trouvés : sites, images, profils ou commentaires…

Exemple concret

Données publiques

- Pseudonyme (Luki_2009)
- Commentaires généraux (YouTube, blog)
- Participation à un jeu ou score
- Vidéos TikTok sans info personnelle directe
- Avis sur application (sans précision personnelle forte)
- Participation à un tournoi (nom uniquement)
- Profil sur plateforme éducative (si limité au prénom)

Données privées

- Nom + prénom complet (Lucas Martin)
- Photo identifiable (visage)
- Âge ou date de naissance
- École identifiable (uniforme, bâtiment)
- Lieu fréquenté (parc, club sportif)
- Géolocalisation (photos, stories)
- Adresse électronique
- Trajets quotidiens
- Liste d'amis
- Intérieur du domicile (vidéo chambre)
- Publications familiales (parents)
- Localisation de vacances en temps réel

Support 1.3 : Analyse de risque données sensibles

Les élèves identifient les informations sensibles et évaluent les risques associés à leur diffusion.

Exemple concret

1. Identité civile (nom, prénom)

- Pourquoi est-ce sensible ? C'est la clé d'entrée principale de l'identité numérique : elle permet d'identifier précisément une personne.
- Risques : facilite l'usurpation d'identité et permet à un tiers de mener une enquête approfondie sur la vie de la personne (recoupement d'informations).

2. Image de soi (photos du visage)

- Pourquoi est-ce sensible ? Cela rend la personne reconnaissable physiquement par n'importe qui.
- Risques : utilisation frauduleuse, détournement d'image (montages) ou reconnaissance dans la vie réelle par des inconnus.

3. État civil (âge / date de naissance)

- Pourquoi est-ce sensible ? C'est une donnée de vérification souvent utilisée pour confirmer une identité ou récupérer un mot de passe.
- Risques : piratage de comptes, ciblage publicitaire agressif, arnaques ou manipulation.

4. Environnement quotidien (école identifiable)

- Pourquoi est-ce sensible ? Cela permet de localiser un lieu où l'on se trouve chaque jour à des heures prévisibles.
- Risques : suivi physique, intrusion dans l'établissement et atteinte à la sécurité personnelle.

5. Localisation instantanée (géolocalisation)

- Pourquoi est-ce sensible ? Elle donne une position géographique exacte (coordonnées GPS, nom d'un parc ou d'une ville).
- Risques : localisation en temps réel par des tiers, fin de l'anonymat et atteinte à la vie privée.

6. Sphère privée (intérieur du domicile)

- Pourquoi est-ce sensible ? Les vidéos ou photos de la chambre ou du salon donnent des informations sur le lieu de vie et le niveau de richesse.
- Risques : cambriolage, intrusion ou identification précise du logement.

7. Communication (adresse électronique)

- Pourquoi est-ce sensible ? C'est le canal qui permet de contacter directement la personne et sert souvent d'identifiant de connexion.
- Risques : réception de spam, tentatives de phishing (hameçonnage) ou piratage de la boîte mail.

8. Habitudes de déplacement (trajets quotidiens)

- Pourquoi est-ce sensible ? Cela révèle des routines fixes (par exemple, le chemin entre l'école et la maison).
- Risques : surveillance accrue et mise en danger physique lors des déplacements.

9. Réseau social (liste d'amis)

- Pourquoi est-ce sensible ? Il donne accès à des informations sur l'entourage, les fréquentations et les relations proches.
- Risques : harcèlement, arnaques en chaîne (rebond) et collecte d'informations sur les proches.

10. Vie familiale (publications de la famille)

- Pourquoi est-ce sensible ? Elle ajoute des informations personnelles sur des tiers (âge des frères/sœurs, événements familiaux).
- Risques : perte de contrôle sur l'image de la famille et diffusion involontaire d'informations privées.

11. Signalement d'absence (vacances en direct)

- Pourquoi est-ce sensible ? Cela indique clairement que le domicile principal est inoccupé.
- Risques : cambriolage et exploitation malveillante de cette information par des personnes malintentionnées.

Support 1.4 : Identification des données

Les élèves analysent une publication (photo ou message) pour distinguer les données visibles et repérer les éléments d'identification, tels que l'image de profil, le pseudonyme ou les publications associées.

Exemple concret

Éléments d'identification directs

Permettent de reconnaître immédiatement une personne.

- Nom et prénom
- Pseudonyme / identifiant (ex. : Luki_2009)
- Photo de profil (visage)
- Vidéos montrant la personne
- Voix (dans des vidéos ou messages audio)

Éléments d'identification indirects

Pris séparément, ils semblent anodins, mais ensemble ils permettent d'identifier quelqu'un.

- Âge ou date de naissance
- École / lieu de travail
- Ville ou quartier
- Club sportif / activité extrascolaire
- Lieux fréquentés (parc, centre commercial…)
- Amis / relations visibles
- Habitudes (trajets, horaires)

Éléments techniques d'identification

Souvent invisibles, mais très révélateurs.

- Adresse électronique
- Nom d'utilisateur/utilisatrice utilisé sur plusieurs sites
- Adresse IP (non visible directement, mais exploitable)
- Données de géolocalisation (GPS, lieux tagués)
- Appareil utilisé (smartphone, modèle)

Éléments contextuels (indices complémentaires)

Permettent de confirmer une identité.

- Publications (photos, commentaires, likes)
- Objets visibles (uniforme, logo d'école, chambre…)
- Évènements (anniversaire, vacances…)
- Style d'écriture ou d'expression
- Réseaux d'amis communs

Support 1.5 : Analyse des données « invisibles »

L'enseignante/l'enseignant révèle ensuite les données invisibles potentielles (date, lieu, appareil, etc.) afin que les élèves puissent compléter leur analyse.

Exemple concret

1. Analyse visuelle (indices de contexte)

Avant d'utiliser la technique, apprenez aux élèves à devenir des « détectives de l'image ». Faites-les réfléchir sur les déductions possibles grâce à :

- L'arrière-plan : lieux reconnaissables, panneaux de signalisation, architecture d'une école
- Les ombres : elles permettent d'estimer le moment de la journée (orientation et longueur)
- Les vêtements : ils indiquent la saison, la météo ou le type d'activité pratiquée

2. Relever les métadonnées : la « carte d'identité » de l'image

Expliquez simplement aux élèves que chaque fichier numérique contient des informations techniques cachées :

- La date et l'heure exactes de la prise de vue
- Le modèle de l'appareil ou du smartphone utilisé
- Le lieu géographique (**coordonnées GPS**) si l'option était activée

3. Comment révéler les métadonnées ?

Sur un ordinateur	**Sur smartphone**
Étapes : 1. Télécharger ou enregistrer l'image 2. Faire un clic droit sur le fichier 3. Cliquer sur « Propriétés » 4. Aller dans l'onglet « Détails » On peut y trouver : • La date de prise de vue • L'appareil photo / smartphone utilisé • Parfois, la localisation GPS	Étapes : 1. Ouvrir la photo dans la galerie 2. Cliquer sur « Informations » ou « Détails » (souvent un « i ») On peut y trouver : • La date de prise de vue • Le lieu (carte parfois affichée) • Le type d'appareil

Support 1.6 : Enquête ou puzzle

Sous forme d'enquête ou de puzzle, les élèves reconstituent le profil d'une personne en s'appuyant sur un ensemble de traces numériques fournies.

Exemple concret

« Qui est Acturus_2011 ? »

Objectif
Reconstituer une identité numérique en croisant des traces éparses et sensibiliser à la protection des données personnelles.

Matériel (à distribuer sous forme de cartes)
Chaque groupe reçoit des « pièces du puzzle ».
(À découper sous forme de cartes d'indices pour les groupes d'élèves.)

Cartes indices (exemples)
1. Photo d'un adolescent avec un maillot de foot (logo « FC Jemeppe »)
2. Capture Instagram : @Acturus_2011
3. Commentaire : « Trop bien l'entraînement ce mercredi ! »
4. Photo d'anniversaire avec « 15 ans 🎂 »
5. Publication d'un parent : « Bravo, Arthur, pour ton match ! »
6. Capture d'écran d'un jeu avec pseudo « Acturus_11 »
7. Photo avec un panneau « École communale Jemeppe Centre »
8. Story : « En route pour les cours 🥱 »
9. Image avec métadonnées (date : mercredi 16h30)
10. Liste d'amis (dont « Maxime foot », « Sarah classe »)

Consignes pour les élèves
En utilisant uniquement les indices ci-dessus, réponds aux questions suivantes :
1. Identité : quel est son prénom ?
2. Âge : quel âge a-t-il réellement ?
3. Éducation : dans quel établissement étudie-t-il ?
4. Loisirs : quelle activité occupe son temps libre ?
5. Localisation : dans quelle ville se trouve-t-il régulièrement ?

Analyse les risques en classant les réponses ci-dessus selon leur dangerosité potentielle :
- Sans risque particulier : informations générales qui ne permettent pas de cibler l'individu
- Sensible / risqué : informations qui, croisées, permettent de localiser ou d'identifier précisément l'élève

Corrigé pour l'enseignant/l'enseignante

Solution de l'enquête

- Prénom : Arthur (révélé par la publication du parent)
- Âge : 15 ans (selon la date de l'indice « 15 ans »)
- Activité : football (maillot, club, entraînement)
- Lieu : Jemeppe (club de foot et nom de l'école)
- École : école communale Jemeppe Centre (clairement identifiable sur la photo)

Analyse des données (exemple de classement)

- Sans risque : le pseudo « Acturus_11 », le fait d'aimer le foot
- Sensible : le prénom réel associé au visage, le nom de l'école (lieu de présence fixe), les horaires d'entraînement (habitudes de déplacement)

Support 1.7 : Enquête ou puzzle

Sous forme d'enquête ou de puzzle, les élèves reconstituent le profil d'une personne en s'appuyant sur un ensemble de traces numériques fournies.

Exemple concret

« Retrouver l'identité d'un internaute »

Objectif
Comprendre comment une identité peut être reconstituée en croisant des traces numériques visibles et invisibles.

Scénario
Une personne publie régulièrement du contenu sous le pseudo « ShadowFox ».

Votre mission
Percer son anonymat et découvrir tout ce qu'il est possible de savoir sur lui à partir de ses traces.

Dossier d'enquête (indices)

- **Indice 1 : profil public**
  › Pseudo : ShadowFox
  › Photo : paysage (aucun visage)
- **Indice 2 : publication**
  › « Encore une journée au top au club 🔥 »
  › Photo d'un terrain de basket
  › Détail visible : panneau « Hall sportif de Seraing »
- **Indice 3 : commentaire d'un ami**
  « Bien joué, Thomas ! »
- **Indice 4 : image téléchargée (avec métadonnées révélées par l'enseignant/l'enseignante)**
  › Date : mardi 18h15
  › Appareil : iPhone
  › Lieu : Seraing
- **Indice 5 : story**
  « Match tous les mardis et jeudis 💪 »
- **Indice 6 : profil secondaire**
  Pseudo similaire « Thomas_Fox » sur un forum
- **Indice 7 : photo**
  Photo d'équipe avec un t-shirt « Basket Club Seraing »

Consignes pour les élèves

À l'aide des indices, répondez aux questions suivantes pour dresser le portrait de l'internaute :

1. Quel est le prénom de cette personne ?
2. Dans quelle ville vit-elle ou se rend-elle très souvent ?
3. Quelle activité pratique-t-elle ?
4. Quels sont ses horaires ou jours de présence réguliers ?
5. Classez les informations trouvées selon qu'elles soient :
   - **Visibles** (directement sur l'image ou le texte)
   - **Invisibles** (cachées dans le fichier technique)
   - **Sensibles** (qui permettent de croiser des informations pour identifier la personne)

Solution attendue

- Prénom : Thomas (identifié via le commentaire et le profil secondaire).
- Ville : Seraing (identifiée via le panneau, les métadonnées et le nom du club).
- Activité : basket (terrain, t-shirt du club).
- Habitudes : entraînements et présence les mardis et jeudis soir (confirmé par la story et l'heure des métadonnées).

Pistes de réflexion

Cet exercice montre que même sans afficher son visage (indice 1), la combinaison d'un lieu (Seraing), d'un prénom (Thomas) et d'un emploi du temps (mardi/jeudi) rend l'anonymat presque impossible à maintenir.

Support 1.8 : Localisation des paramètres de confidentialité

Les élèves observent différentes interfaces pour localiser les paramètres de confidentialité et expliquer leur utilité.

Exemple concret

« Retrouver l'identité d'un internaute »

Service	Chemin d'accès aux paramètres de confidentialité
Facebook	Menu › Paramètres et confidentialité › Paramètres › Confidentialité
Microsoft	Paramètres › Confidentialité › Tableau de bord
Google	Paramètres › Données et confidentialité
Instagram	Profil › Menu › Paramètres et confidentialité › Confidentialité
PlayStation (PSN)	Paramètres › Gestion du compte › Paramètres de confidentialité
WhatsApp	Paramètres › Confidentialité
Snapchat	Profil › Paramètres › sections Confidentialité / Qui peut…
YouTube	YouTube › Photo de profil › Gérer votre compte Google › Données et confidentialité › Paramètres YouTube (historique, pub, confidentialité)
Spotify	Paramètres › Confidentialité et partage

Mettre en évidence le symbole ⚙ **« engrenage », typique du menu « paramètres »** dans de nombreux outils ou applications.

Support 1.9 : Synthèse des bonnes pratiques

Une mise en commun permet de synthétiser les bonnes pratiques pour protéger son identité numérique.

Exemple concret

1. Limiter les informations personnelles
- Garder pour soi son nom complet, son adresse précise, son établissement scolaire ou son numéro de téléphone…
- Éviter de publier sa date de naissance ou ses habitudes

2. Choisir un pseudonyme neutre
Opter pour un pseudonyme neutre qui ne contient ni le vrai nom, ni l'âge, ni la localisation (ex: éviter Luki_2009)

3. Faire attention aux photos et vidéos
- Avant de publier, vérifier que le domicile, l'école ou des objets personnels identifiables ne sont pas visibles
- Demander l'accord avant de publier la photo ou une vidéo de quelqu'un

4. Gérer la trace géographique
- Désactiver la géolocalisation automatique
- Ne pas partager sa position en direct
- Ne jamais partager sa position en direct et supprimer les « tags » de lieux sur les publications passées

5. Paramétrer la confidentialité
- Mettre ses comptes en mode « privé »
- Vérifier régulièrement les paramètres pour choisir qui peut voir, commenter ou partager

6. Réfléchir avant de publier
- Se poser la question : "Est-ce que je veux que tout le monde voie ça ?"
- Penser que ce qui est publié peut rester longtemps

7. Faire attention aux données invisibles
- Se méfier des métadonnées cachées dans les photos (date, lieu…)
- Supprimer les métadonnées si nécessaire

8. Contrôler son réseau
- N'accepter que des personnes connues
- Développer un esprit critique face aux faux profils et aux usurpations d'identité

9. Être vigilant face aux risques

- Ne pas répondre à des messages suspects
- Ne jamais partager ses mots de passe
- Signaler un contenu ou un comportement problématique

Message clé à retenir

« Protéger son identité numérique, c'est réfléchir avant de publier et garder le contrôle total de ses informations. »

Maitriser ses données et sa présence en ligne

Objectifs : comprendre la circulation des données, les enjeux de leur collecte (y compris par l'IA) et apprendre à paramétrer et protéger son compte.

Support 2.1 : Classification de données

Les élèves reçoivent une liste d'informations (photo, âge, localisation, contacts, etc.) qu'ils répartissent entre données publiques et privées. Ils justifient ensuite leurs choix en groupe, puis confrontent leurs réponses avec celles de leurs camarades.

Exemple concret

- Nom et prénom
- Pseudonyme
- Photo de profil / Avatar
- Adresse électronique
- Mot de passe
- Âge
- Date de naissance
- Ville de résidence
- Adresse complète
- Numéro de téléphone
- École fréquentée
- Loisirs
- Liste d'amis
- Publications (photos, vidéos)
- Localisation en temps réel
- Historique de navigation
- Messages privés
- Centres d'intérêt (pages likées)
- Adresse IP
- Cookies
- Position GPS
- Identifiant de l'appareil

Informations plutôt publiques (partageables sous conditions)	Informations plutôt privées (à garder sous contrôle)
Pseudonyme	Nom et prénom (selon contexte)
Photo de profil (si avatar)	Adresse électronique
Âge (approximatif)	Mot de passe
Ville de résidence	Date de naissance complète
Loisirs	Adresse complète
Centres d'intérêt	Numéro de téléphone
Publications (selon paramètres)	École fréquentée
Liste d'amis (selon paramètres)	Localisation en temps réel
Spotify	Messages privés
	Historique de navigation
	Adresse IP
	Cookies
	Position GPS
	Identifiant de l'appareil
	Photo de profil (si vraie photo)

Support 2.2 : Analyse des données

Les élèves analysent diverses situations (création de comptes, publication, formulaire) pour identifier les données transmises volontairement par l'utilisateur.

Exemple concret

Situation 1 : Création d'un compte sur un réseau social
Données fournies volontairement : nom, prénom, adresse électronique, mot de passe, date de naissance, photo de profil ou avatar, centres d'intérêt

Remarque : ces informations sont généralement demandées par les plateformes pour créer un profil identifiable et personnalisé. L'utilisateur/l'utilisatrice choisit en partie ce qu'il communique et en est responsable.

Situation 2 : Publication d'une photo sur Instagram ou TikTok
Données fournies volontairement : photo, légende, hashtags, localisation (si activée), tags d'amis

Remarque : l'utilisateur/l'utilisatrice décide de partager la photo et les informations qui l'accompagnent. Les hashtags et tags sont ajoutés volontairement pour rendre la publication visible à un certain public.

Situation 3 : Remplissage d'un formulaire en ligne pour un concours
Données fournies volontairement : nom, prénom, âge, adresse électronique, numéro de téléphone, réponses au questionnaire

Remarque : l'utilisateur/l'utilisatrice complète le formulaire pour participer et insère ces données de manière consciente.

Situation 4 : Inscription à une infolettre
Données fournies volontairement : prénom, adresse électronique, préférences (thèmes souhaités)

Remarque : l'utilisateur/l'utilisatrice choisit de s'inscrire et indique les informations nécessaires pour recevoir le contenu ciblé.

Situation 5 : Création d'un profil sur un site de jeux en ligne
Données fournies volontairement : pseudo, âge, mot de passe, avatar, centre d'intérêt (jeux favoris)

Remarque : ces données, toutes fournies volontairement, permettent de personnaliser l'expérience de jeu et de créer un compte sécurisé.

Situation 6 : Remplissage d'un formulaire de commande en ligne
Données fournies volontairement : nom, prénom, adresse de livraison, adresse électronique, numéro de téléphone, mode de paiement.

Remarque : ces informations sont nécessaires pour recevoir la commande.

Situation 7 : Publication d'un avis sur un produit sur un site (e-commerce, streaming…)
Données fournies volontairement : note, commentaire, pseudo, photo (optionnelle), date d'achat (si demandée), produit acheté, média visionné/écouté…

Remarque : l'utilisateur/l'utilisatrice rédige lui-même l'avis, mais parfois son profil est visible de tous les utilisateurs/utilisatrices qui ont accès à cet avis.

Support 2.3 : Observation des données

À partir de situations concrètes, les élèves découvrent les données collectées automatiquement, telles que les cookies ou la géolocalisation.

Exemple concret

Situation 1 : Je me connecte à un site internet
Données collectées automatiquement : cookies, adresse IP, type de navigateur, système d'exploitation…

Situation 2 : Je visite un site e-commerce
Données collectées automatiquement : cookies de suivi (pages vues, produits consultés), durée de navigation, clics sur les boutons.

Situation 3 : J'utilise une application météo
Données collectées automatiquement : localisation (GPS - réseau), type d'appareil, identifiant de l'appareil, date d'utilisation…

Situation 4 : Je regarde des vidéos sur une plateforme en ligne
Données collectées automatiquement : durée de visionnage, vidéos consultées, interactions (like, pause, avance rapide), commentaires ajoutés…

Situation 5 : J'effectue des exercices avec une application de suivi d'activité
Données collectées automatiquement : nombre de pas, distance parcourue, fréquence cardiaque (capteurs du téléphone ou montre connectée), géolocalisation…

Situation 6 : J'utilise un moteur de recherche
Données collectées automatiquement : historique de recherche, adresse IP, type de navigateur, sites consultés…

Situation 7 : J'ouvre une application d'achat en ligne
Données collectées automatiquement : identifiant de l'appareil, clics sur les produits, durée de consultation, produits regardés, habitudes d'achat…

Situation 8 : Je me connecte à un réseau Wi-Fi public
Données collectées automatiquement : adresse MAC de l'appareil, localisation approximative, sites consultés, quantité de données utilisées…

Situation 9 : Je navigue sur un réseau social sans publier
Données collectées automatiquement : pages consultées, interactions avec le fil d'actualité, temps passé sur chaque publication, cookies de suivi…

Support 2.4 : Identification des accès aux données

À partir d'un scénario (publication d'une photo), les élèves identifient toutes les personnes ou organisations pouvant y accéder.

Exemple concret

Scénario 1 : Le cahier de classe

- Action : tu dessines dans ton cahier et tu le montres à ton voisin
- Qui peut voir ? Toi + ton voisin

Idée clé : accès très limité et contrôle total.

Scénario 2 : Le couloir de l'école

- Action : ta photo est affichée dans le couloir
- Qui peut voir ? Élèves d'autres classes + enseignants + visiteurs

Idée clé : public élargi, mais limité aux murs de l'école.

Scénario 3 : Groupe de classe ou statut « privé »

- Action : tu publies dans un groupe scolaire ou tu sélectionnes tes accès
- Qui peut voir ? Les membres choisis (amis, élèves, professeurs)

Idée clé : cercle fermé, mais la photo peut être enregistrée ou transférée.

Scénario 4 : Groupe privé en ligne

- Action : tu publies une photo dans un groupe de classe (réseau social ou environnement numérique scolaire)
- Qui peut voir ? Les membres du groupe (élèves + parfois enseignants)

Idées clé :
› accès contrôlé, mais numérique. Attention, les captures d'écran restent possibles !
› impression de sécurité, mais pas totale.

Scénario 5 : Publication publique sur un réseau social

- Action : tu publies une photo en statut « public »
- Qui peut voir ? Amis/abonnés + personnes inconnues + entreprises + parfois tout Internet

Idée clé : accès très large et difficile à contrôler.

Scénario 6 : Le groupe WhatsApp familial

- Action : tu partages une photo dans un groupe familial
- Qui peut voir ? Tous les membres du groupe. Ils peuvent l'enregistrer ou la repartager

Idée clé : cercle « fermé », mais diffusion possible.

Scénario 7 : Le « statut » privé

- Action : tu publies une photo en statut « privé » et tu sélectionnes qui peut y accéder
- Qui peut voir ? Les personnes sélectionnées uniquement (mais capture d'écran possible)

Idée clé : impression de sécurité, mais pas totale.

Scénario 8 : Le partage par une amie

- Action : tu envoies une photo à une amie… qui la republie
- Qui peut voir ? Les amis de ton amie. Peut-être des personnes inconnues

Idée clé : perte de contrôle sur la diffusion.

Scénario 9 : La recherche sur Internet

- Action : ta photo est publiée publiquement et apparaît dans un moteur de recherche
- Qui peut voir ? Toute personne qui fait une recherche. Même des personnes que tu ne connais pas

Idée clé : visibilité très large et durable.

Variantes pour enrichir l'activité

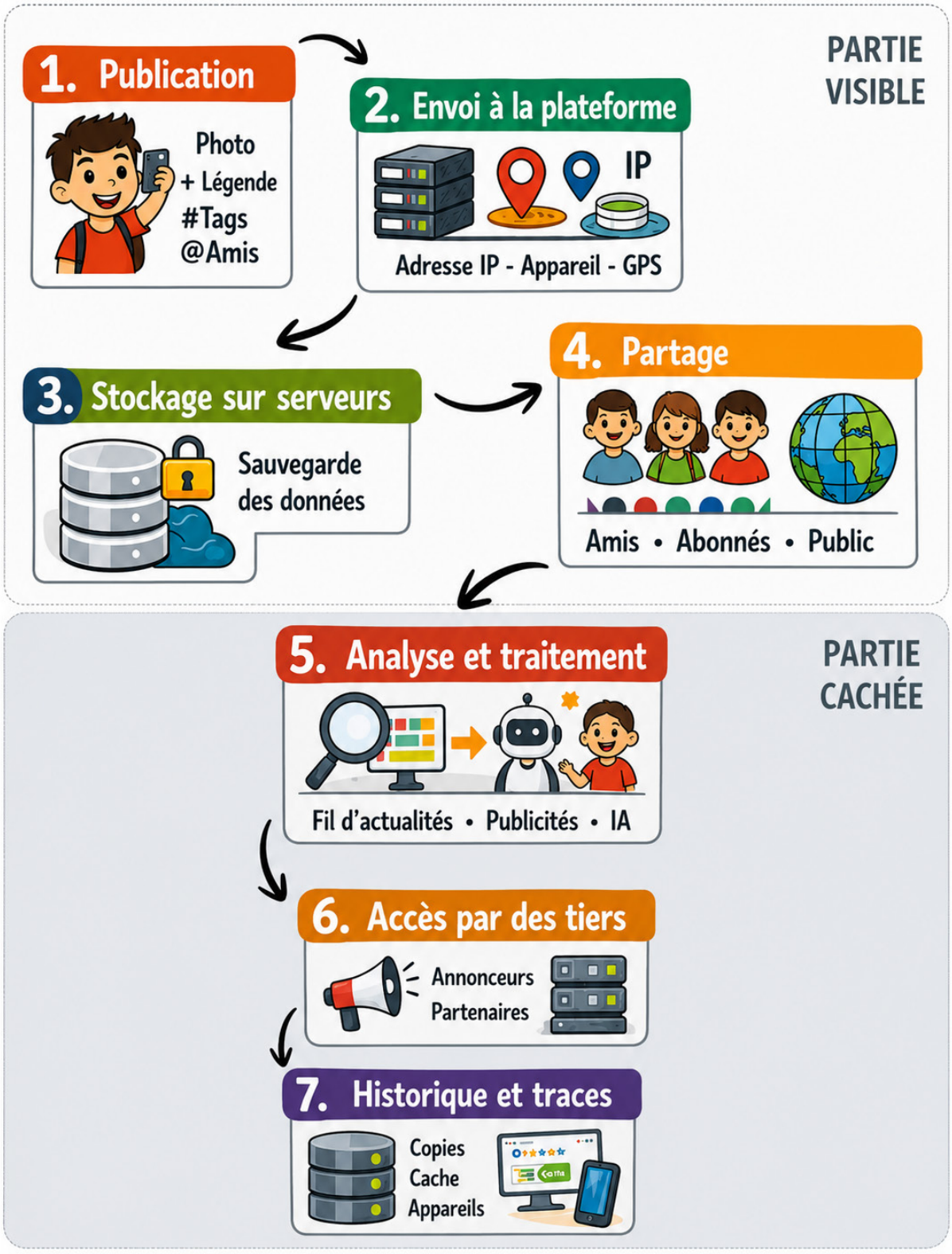
Il est possible de poser à chaque scénario les questions suivantes :

- Qui peut voir maintenant ?
- Qui pourrait voir plus tard ?
- Peut-on contrôler celui qui voit ?
- Celui qui voit peut-il contrôler ?

Support 2.5 : Schématisation du parcours des données

Les élèves réalisent un schéma du parcours de la donnée pour visualiser son cheminement entre les différents acteurs : amis/amies, plateformes, annonceurs ou moteurs de recherche.

Exemple concret



AI *Image réalisée avec l'intelligence artificielle.*

Support 2.6 : Schématisation du parcours des données

Les élèves réalisent un schéma du parcours de la donnée pour visualiser son cheminement entre les différents acteurs : amis/amies, plateformes, annonceurs ou moteurs de recherche.

Exemple concret

1. Création / publication de la donnée : l'intention de l'élève
L'élève prend une photo et la publie avec une légende et éventuellement des tags.
Données ajoutées volontairement : photo, texte, hashtags, localisation, tags d'amis.

2. Transmission à la plateforme
La photo et ses métadonnées (date, lieu, appareil) sont envoyées au serveur de la plateforme.
Données collectées automatiquement : adresse IP, type d'appareil, cookies, parfois localisation GPS.

2. Stockage sur les serveurs
La plateforme enregistre la photo et les informations associées dans sa base de données.
Conséquence technique : Ces données sont sauvegardées pour un usage futur (sauvegarde, analyse, recommandations).

3. Partage avec le réseau
Selon les paramètres de confidentialité, la photo peut être vue par un public défini (amis, abonnés, ou public.
Données visibles pour d'autres utilisateurs/utilisatrices : photo, légende, hashtags, tags.

4. Analyse et traitement par la plateforme
La plateforme analyse la photo et les métadonnées pour :

- Personnaliser le fil d'actualité
- Proposer des publicités ciblées
- Entraîner des systèmes automatisés (IA pour reconnaissance faciale, suggestions d'amis, etc.)

5. Accès par des tiers
Certaines données peuvent être transmises à des :

- Annonceurs pour publicité ciblée
- Partenaires analytiques pour statistiques d'usage ; moteurs de recherche si la publication est publique

6. Historique et traces
Même après suppression par l'utilisateur/l'utilisatrice, des copies peuvent rester :

- Sur les serveurs de la plateforme
- Dans les caches des moteurs de recherche
- Sur des appareils ayant déjà consulté la publication

Support 2.7 : Classification de données

Les élèves discutent des finalités de la collecte de données (publicité, personnalisation, entraînement des IA, etc.) et les répartissent en deux catégories : les usages utiles et les usages problématiques.

Exemple concret

Gestion et sécurité du compte

- Créer et gérer un compte pour permettre à l'utilisateur/l'utilisatrice d'exister sur la plateforme
- Vérifier l'identité pour éviter les faux comptes ou les usurpations
- Sécuriser les comptes pour assurer une protection contre le piratage
- Permettre la connexion automatique afin d'éviter de se reconnecter plusieurs fois

Personnalisation de l'expérience utilisateur

- Personnaliser le contenu pour afficher des publications adaptées aux goûts de chacun
- Recommander des contenus pour proposer des vidéos, des pages ou des profils similaires
- Géolocaliser l'utilisateur/l'utilisatrice pour proposer des contenus ou des services de proximité
- Envoyer des notifications pour informer des nouveaux messages ou des nouveautés
- Proposer des amis/amies ou contacts pour connecter les utilisateurs/les utilisatrices entre eux/elle

Optimisation et amélioration technique

- Améliorer les services pour rendre l'application plus efficace et agréable
- Corriger les bugs pour résoudre les problèmes techniques rencontrés
- Adapter l'affichage à l'appareil utilisé (téléphone, tablette ou ordinateur)
- Entraîner des systèmes automatisés (IA) pour améliorer les suggestions ou la reconnaissance d'images

Publicité et modèle économique

- Afficher des publicités ciblées en lien avec les intérêts de l'utilisateur/l'utilisatrice
- Financer le service grâce à la publicité ou à l'utilisation des données
- Partager des données avec des partenaires pour des analyses ou des services complémentaires

Analyse, statistiques et modération

- Comprendre les habitudes d'utilisation pour savoir quand et comment le service est utilisé
- Mesurer l'audience pour connaître le nombre de personnes utilisant la plateforme
- Analyser les tendances pour identifier ce qui est populaire
- Modérer les contenus pour repérer et supprimer les éléments inappropriés

Montrer que :

- Les données ont plusieurs usages
- Certains usages sont utiles
- D'autres usages peuvent poser des questions sur la vie privée

Support 2.8 : Paramétrage de confidentialité

Les élèves accèdent à un compte fictif ou à des captures d'écran pour explorer les paramètres de confidentialité. Ils modifient ensuite ces réglages afin de limiter l'accès à leurs informations personnelles.

Exemple concret

Accéder aux paramètres	Sur la plupart des réseaux sociaux : 1. Aller sur son « **profil** » 2. Cliquer sur « Paramètres » ou « Confidentialité » 3. Chercher la section : • « Vie privée » • « Sécurité »
Gérer qui peut voir les publications	**A. Rendre un compte privé** Permet de limiter l'accès aux abonnés acceptés. Activer : « Compte privé » Résultat : seules les personnes acceptées voient les publications.
	B. Choisir le public d'une publication Pour chaque publication, choisir : • « Public » • « Amis » • « Moi uniquement »
Gérer les identifications (tags)	Activer « Validation des identifications ». Résultat : il faut accepter avant que la photo apparaisse sur le profil.
Désactiver la localisation	Aller dans « Paramètres du téléphone », puis « Localisation ». Désactiver ou limiter l'accès de l'application.
Gérer les messages et commentaires	Limiter l'accès aux messages seulement aux amis. Filtrer les commentaires. Bloquer ou signaler si nécessaire.

Gérer les données et le suivi	Publicités ciblées ou suivi de ta navigation en ligne. Actions : • Refuser les cookies non essentiels • Désactiver la personnalisation des pubs (si possible) • Vérifier les autorisations des applications • Si besoin, installer un bloqueur de publicités
Avant de publier : les bons réflexes	Toujours se demander : • Qui peut voir cette publication ? • Est-ce que je veux que tout le monde la voie ? • Est-ce que cela concerne quelqu'un d'autre ?

Support 2.9 : Suppression de ses traces sur un appareil partagé

Les élèves identifient les actions nécessaires pour effacer leurs traces sur un appareil partagé, telles que la déconnexion des comptes, la suppression de l'historique et le nettoyage des cookies.

Exemple concret

À faire systématiquement

- Se déconnecter de tous ses comptes (réseaux sociaux, messageries, applications y compris si besoin dans les navigateurs) pour empêcher une autre personne d'agir en votre nom
- Vérifier et fermer les sessions des comptes connectés automatiquement, comme les comptes Google ou Microsoft
- Supprimer les mots de passe éventuellement enregistrés dans le navigateur (Chrome, Edge, Firefox…) et éviter de les enregistrer sur un appareil public à l'avenir :
  › Ouvrir les paramètres
  › Aller dans « Mots de passe enregistrés »
  › Supprimer ceux enregistrés

Pourquoi ? Sinon, la personne suivante pourrait accéder à ton compte et agir en ton nom.

Effacer les traces de navigation

- Accéder aux paramètres du navigateur pour effacer l'historique navigation :
  › Ouvrir les paramètres
  › Cliquer sur « Historique »
  › Choisir « Effacer les données de navigation » (y compris les cookies)
- Utiliser le mode « navigation privée » ou « incognito » dès le début de la session pour limiter l'enregistrement automatique des données
  Avantage : moins de traces enregistrées automatiquement et effacement des données à la fermeture
- Fermer tous les onglets du navigateur ainsi que les applications restées ouvertes avant de quitter l'appareil

Pourquoi ? Sinon ils restent accessibles aux autres.

Supprimer les fichiers et les contenus créés

- Vider le dossier « Téléchargements » pour supprimer les documents ou images
- Effacer les photos, vidéos ou fichiers audios personnels enregistrés sur l'appareil
- Désinstaller les applications qui ont été ajoutées pour un usage ponctuel et supprimer les comptes invités, notamment sur les tablettes partagées

Pourquoi ? Sinon ils restent accessibles à d'autres personnes.

Sur une tablette partagée, penser aussi à :

- Supprimer les comptes ajoutés
- Désinstaller les applications non nécessaires
- Vérifier et éventuellement supprimer les photos, vidéos ou audios enregistrés

2 Gérer son profil et ses actions
Propositions d'activités

Attendus visés

- **Compétence** : Gérer son identité numérique, ses traces, ses données personnelles, de manière responsable
- **Savoir** : Utiliser, adéquatement en contexte, les termes dont profil, protection de la vie privée
- **Savoir** : Identifier et reconnaitre les avantages de la gestion de son identité numérique en termes de préservation de ses droits et de responsabilité

Exemples d'activités

Enquête guidée sur une identité numérique

Objectifs : comprendre comment se construit un profil et ce qu'il révèle.

Déroulement de l'activité :

- **Analyse d'un profil fictif (Support 1.1)**
  En groupes, les élèves analysent un profil fictif à l'aide d'un questionnaire guidé afin de différencier les informations explicites des données déduites. Ils identifient les éléments relevant de la vie privée avant de recouper les différentes traces numériques pour reconstituer l'identité globale de la personne.
- **Comparaison des déductions (Support 1.2)**
  Les élèves comparent leurs déductions d'abord entre eux, puis à celles listées par l'enseignante/l'enseignant reprenant des hypothèses simples : centres d'intérêt, tranche d'âge, habitudes, localisation ou préférences, à partir d'indices visibles (likes, photos, horaires…). L'enseignante/l'enseignant met en évidence que certaines informations sont facilement déductibles, même à partir de peu de données. Elle/il souligne enfin que ce type d'analyse est automatisé dans de nombreux services numériques, d'où l'importance de gérer correctement son identité numérique.
- **Identification des risques (Support 1.3)**
  Les élèves évaluent les enjeux d'une identité numérique maîtrisée en identifiant les risques de dérives et les avantages stratégiques, tels que la protection de la vie privée et la gestion de la réputation.
- **Formulation de principes concrets (Support 1.4)**
  L'activité débouche sur la formulation de principes concrets pour mieux maîtriser ses publications et limiter la diffusion de données personnelles.

Le parcours des données et les bons réflexes

Objectif : comprendre la circulation des données et adopter un comportement responsable.

Déroulement de l'activité :

- **Tri de cartes en groupes (Support 2.1)**
  Par groupes, les élèves reçoivent des cartes « actions » (ex. : publier une photo, liker une page, activer la localisation, accepter les cookies) et doivent les classer en « données fournies » ou « données collectées ». Terminer avec une correction collective avec justification.
- **Évaluation de l'impact des interactions numériques (Support 2.2)**
  Les élèves étudient des publications (photos de groupe, commentaires, partages) via un questionnaire ciblé pour évaluer l'impact de chaque interaction numérique.
- **Synthèse des bonnes pratiques (Support 2.3)**
  Les élèves co-construisent une synthèse des bonnes pratiques, suivie d'un choix individuel de trois actions concrètes à appliquer durant le mois pour renforcer leur protection numérique.

Ressources

Pour approfondir le sujet ou compléter ces activités avec des exercices, vous trouverez des ressources gratuites sur :
e-classe.be/numerique-s1-securite

Enquête guidée sur une identité numérique

Objectifs : comprendre comment se construit un profil et ce qu'il révèle.

Support 1.1 : Analyse d'un profil fictif

En groupes, les élèves analysent un profil fictif à l'aide d'un questionnaire guidé afin de différencier les informations explicites des données déduites. Ils identifient les éléments relevant de la vie privée avant de recouper les différentes traces numériques pour reconstituer l'identité globale de la personne.

Exemple concret

Profils	Publications	Infos « visibles »	Éléments déductibles
« Max_foot10 »	• Photo en tenue de foot : « Match gagné 3-1 💪⚽ #Victoire » • Selfie devant une école : « Encore en retard 😅 » • Likes : pages de clubs de football, équipement sportif	Âge : 13 ans Ville : Liège	Pratique le football, est élève, habite Liège. C'est un garçon. **Déductions possibles :** joue en club, va à l'école proche de chez lui…
« Lina_crea »	• Dessin partagé : « Mon nouveau personnage 🖍️✨» • Photo d'un bureau avec tablette graphique • Likes : dessin, manga, tutoriels YouTube	Pas d'âge indiqué. Avatar artistique.	Aime dessiner. Utilise des outils numériques. **Déductions possibles :** probablement une fille ou une femme, plutôt créative, suit des artistes…

Profils	Publications	Infos « visibles »	Éléments déductibles
« TravelTom »	• Photo d'un avion : « Direction les vacances ! » • Photo plage : « Enfin le soleil ☀️ » • Localisation activée (Espagne)	Ville : Barcelone	En voyage à Barcelone. A voyagé en avion. **Déductions possibles :** voyage en famille, pas chez lui actuellement donc maison vide…
« Sarah_fit »	• Photo jogging : « 5 km ce matin 💪 » • Petit déjeuner : « #Healthy life 🥝 » • Likes : sport, fitness, recettes	Âge : 12 ans	Fait du sport, mange équilibré. **Déductions possibles :** s'appelle Sarah, elle court régulièrement, lieux où elle court (d'après ses photos)
« GamerX_ dark »	• Capture d'écran de jeu : « Niveau 50 atteint ! » • Publication à 23h30 • Likes : jeux vidéo, streaming	Ni âge ni localisation	Joue beaucoup. **Déductions possibles :** joue tard, temps d'écran important

Questions guidées pour les élèves

1. Compréhension directe
- Quelles informations sont clairement visibles ?
- Que fait cette personne ?
- Quels sont ses centres d'intérêt ?

2. Déduction
- Que peux-tu deviner sans que ce soit explicitement écrit ?
- Quels indices t'aident à faire ces suppositions ?
- Ces informations sont-elles sûres à 100 % ?

3. Vie privée
- Y a-t-il des informations personnelles ou sensibles ?
- Cette personne partage-t-elle trop d'informations ?
- Quels risques peut-il y avoir ?

4. Réflexion critique
- Cette personne montre-t-elle une image réaliste d'elle-même ?
- Quelles informations pourraient être utilisées par quelqu'un d'inconnu ?

5. Amélioration du profil
- Que faudrait-il éviter de publier ?
- Que faudrait-il modifier pour protéger sa vie privée ?

Support 1.2 : Comparaison des déductions

Les élèves comparent leurs déductions d'abord entre eux, puis à celles listées par l'enseignante/l'enseignant reprenant des hypothèses simples : centres d'intérêt, tranche d'âge, habitudes, localisation ou préférences, à partir d'indices visibles (likes, photos, horaires…).
L'enseignante/l'enseignant met en évidence que certaines informations sont facilement déductibles, même à partir de peu de données. Elle/il souligne enfin que ce type d'analyse est automatisé dans de nombreux services numériques, d'où l'importance de gérer correctement son identité numérique.

Exemple concret

Indices visibles (données)	Ce que le système pourrait déduire
Photos de sport	Aime le sport / pratique une activité physique
Likes sur pages de football, fitness…	Centres d'intérêt orientés « sports »
Photos de dessins, créations	Intérêt pour l'art et la créativité
Likes sur jeux vidéo	Intérêt pour les jeux vidéo
Publications le soir (22h-23h)	Utilise les réseaux le soir
Publications le matin	Actif avant l'école
Photo devant une école	Probablement un élève de cette école
Photos avec amis	Vie sociale active
Localisation activée	Lieu fréquenté / lieu de vie
Photos de vacances	Aime voyager / absent de chez lui
Hashtags (#food, #sport…)	Centres d'intérêt spécifiques
Type d'appareil (smartphone, tablette…)	Niveau d'équipement

Important
Les données partagées délibérément sont extraites par des systèmes d'intelligence artificielle pour profiler les utilisateurs, prédire leurs comportements et personnaliser les services. Bien que ces déductions soient automatisées, elles restent des hypothèses fondées sur des indices visibles et ne reflètent pas toujours la vérité. Cette analyse systématique rend la maîtrise des traces numériques indispensable pour protéger sa vie privée.

Support 1.3 : Comparaison des déductions

Les élèves évaluent les enjeux d'une identité numérique maîtrisée en identifiant les risques de dérives et les avantages stratégiques, tels que la protection de la vie privée et la gestion de la réputation.

Exemple concret

Pistes pour identifier les avantages d'une identité numérique bien gérée

1. Bonne réputation en ligne
L'élève publie des projets scolaires, des réussites ou des activités positives.
Cela peut donner une image sérieuse et fiable, utile pour plus tard (études, emploi).

2. Valorisation de ses compétences
L'élève partage des dessins, vidéos, projets ou participations à des activités.
Cela permet de montrer ce que l'on sait faire et de se démarquer.

3. Protection de sa vie privée
L'élève ne publie pas son adresse ou ses informations personnelles.
Cela limite les risques d'usurpation d'identité ou de harcèlement.

4. Meilleur contrôle de ses données
L'élève vérifie les paramètres de confidentialité de son compte sur un réseau social.
Cela limite qui peut voir ses publications, ses informations…

5. Crédibilité et confiance
L'élève publie des informations vérifiées et respectueuses.
Les autres utilisateurs font davantage confiance à ce profil.

Pistes pour identifier les risques d'une identité numérique mal gérée

1. Mauvaise réputation
L'élève publie des propos insultants ou des contenus inappropriés.
Ces contenus peuvent être vus par beaucoup de personnes et rester longtemps visibles.

2. Atteinte à la vie privée
L'élève partage sa localisation en temps réel ou des photos personnelles.
Cela peut permettre à des inconnus d'obtenir des informations sensibles.

3. Cyberharcèlement
L'élève reçoit des messages moqueurs ou agressifs à la suite d'une publication.
Certaines informations exposées peuvent être utilisées contre la personne.

4. Exploitation des données personnelles
Les plateformes utilisent les likes et recherches pour cibler des publicités.
Vos comportements en ligne sont analysés pour influencer vos choix.

5. Difficulté à effacer ses traces
Une photo supprimée peut avoir été enregistrée ou partagée ailleurs.
Une fois en ligne, une information peut circuler durablement.

6. Jugements rapides et stéréotypes
L'élève déduit les goûts ou la personnalité d'une personne à partir de quelques publications.
Les informations en ligne donnent une image souvent incomplète, voire fausse.

Support 1.4 : Formulation de principes concrets

L'activité débouche sur la formulation de principes concrets pour mieux maitriser ses publications et limiter la diffusion de données personnelles.

Exemple concret

1. Réfléchir avant de publier
Une photo drôle entre amis peut devenir gênante si elle devient incontrôlable.
Une publication peut être copiée, partagée et rester longtemps en ligne.

2. Limiter les informations personnelles
Adresse, numéro de téléphone, école, emploi du temps, lieu en temps réel.
Ces informations peuvent être utilisées à mauvais escient.

3. Paramétrer la confidentialité sur ses comptes
Rendre un compte privé ou limiter l'accès aux amis.
Éviter que des inconnus accèdent aux contenus.

4. Demander l'autorisation avant de publier sur les autres
Demander aux autres avant de poster une photo de groupe.
Respecter la vie privée et le droit à l'image.

5. Faire attention aux applications et sites utilisés
Une application qui demande accès aux contacts ou à la localisation.
Certaines plateformes collectent beaucoup de données non nécessaires à leur fonctionnement.

6. Ne pas tout croire ni tout partager
Éviter de partager une rumeur ou une info douteuse.
Protéger sa crédibilité.

7. Se déconnecter des appareils partagés
Sur un ordinateur de l'école ou d'un ami.
Éviter que quelqu'un accède à ses comptes.

8. Gérer les paramètres de localisation
Ne pas publier sa position en direct.
Éviter d'être suivi ou localisé.

9. Signaler et bloquer si nécessaire
Bloquer un utilisateur ou signaler un contenu.
Se protéger du harcèlement ou des abus.

Le parcours des données et les bons réflexes

Objectif : comprendre la circulation des données et adopter un comportement responsable.

Support 2.1 : Tri de cartes en groupes

Par groupes, les élèves reçoivent des cartes « actions » (ex. : publier une photo, liker une page, activer la localisation, accepter les cookies) et doivent les classer en « données fournies » ou « données collectées ». Terminer avec une correction collective avec justification.

Exemple concret

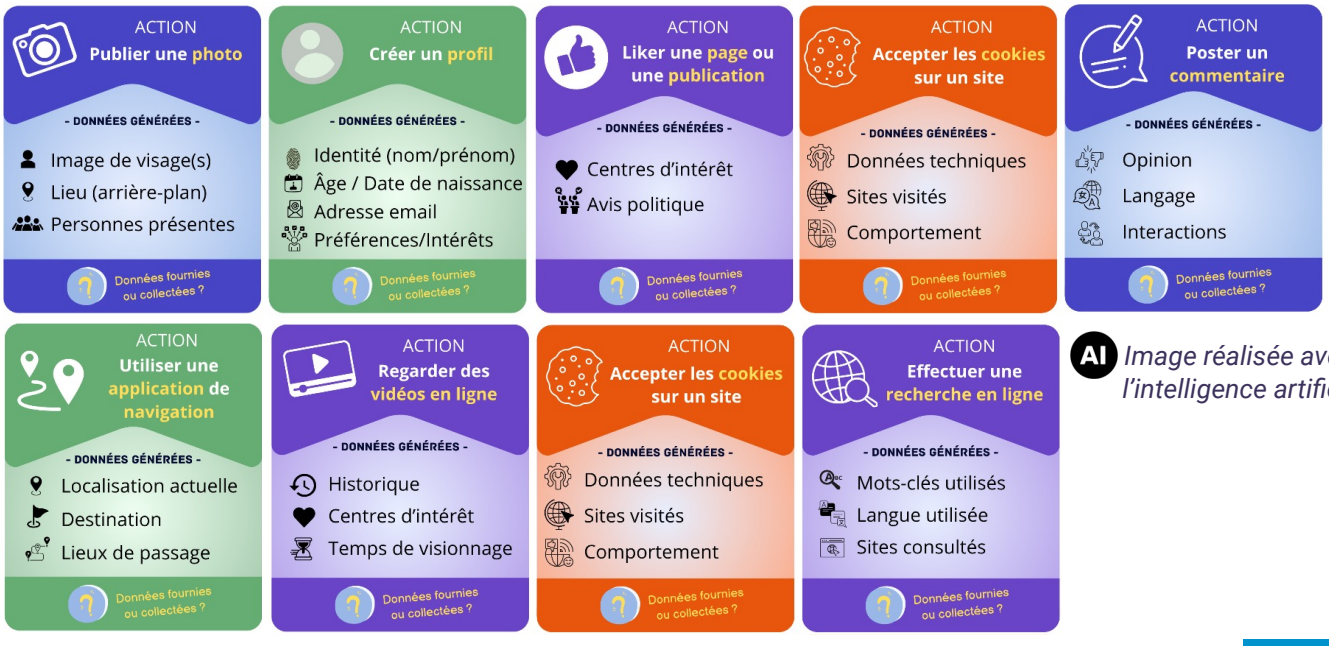
« Données fournies ou collectées ? »

À prévoir

- Des cartes « actions » (réalisées sur PowerPoint, Canva ou autre outil de création) pour ouvrir le débat.
- 3 zones de classement (à poser sur une table ou au tableau) :
  › Données fournies volontairement
  › Données collectées invisiblement
  › Les deux

On distingue deux grandes catégories de données qui alimentent notre identité numérique :

- Les données fournies volontairement : ce sont les informations que l'utilisateur choisit de partager. Cependant, une distinction majeure s'impose : certaines sont publiques (photos, commentaires), tandis que d'autres restent privées pour les autres usagers (date d'anniversaire, adresse électronique, numéro de téléphone). Il est crucial de comprendre que, même si elles ne sont pas visibles par le public, ces données sont bien récoltées et exploitées par les services numériques.
- Les données collectées invisiblement : il s'agit des traces laissées automatiquement lors de la navigation (historique de recherche, temps passé sur une publication, cookies, géolocalisation). Ces informations échappent souvent à la conscience de l'utilisateur.



AI *Image réalisée avec l'intelligence artificielle.*

Support 2.2 : Évaluation de l'impact des interactions numériques

Les élèves étudient des publications (photos de groupe, commentaires, partages) via un questionnaire ciblé pour évaluer l'impact de chaque interaction numérique.

Exemple concret

Situation 1
Sans demander l'avis des autres, Lucas publie une photo de groupe prise pendant la pause à l'école. Sur l'image, plusieurs élèves apparaissent clairement, dont certains font des grimaces. Il ajoute la légende : « Les clowns de la classe 😂».

Situation 2
Sofia commente une vidéo en ligne en écrivant : « Franchement, c'est nul, tu devrais arrêter ». Elle ne connaît pas la personne qui a publié la vidéo.

Situation 3
Amine partage un article trouvé sur un réseau social avec le message : « Incroyable ! Regardez ça ! ». Il n'a pas lu l'article en entier, qui contient en réalité des informations fausses sur une célébrité.

Situation 4
Chloé publie une story dans laquelle elle indique qu'elle est en vacances à l'étranger pour deux semaines, avec une photo devant sa maison avant son départ.

Situation 5
Nathan crée un compte sur une application et renseigne son vrai nom, sa date de naissance, son école et ses centres d'intérêt sans vérifier les paramètres de confidentialité.

Situation 6
Inès envoie une photo de Thomas en train de dormir en classe dans un groupe de discussion privé. La photo est ensuite partagée par d'autres élèves sans son accord, et à l'insu de Thomas.

Situation 7
Tom utilise une application gratuite pour modifier ses photos. Comme il n'a pas lu les règles d'utilisation de l'application, celle-ci accède à sa galerie, à sa localisation et à des noms de contacts identifiés dans ses photos.

Situation 8
Emma regarde plusieurs vidéos sur le sport sur une plateforme. Le lendemain, elle remarque que toutes les vidéos proposées sont liées au sport et qu'elle voit des publicités pour des vêtements de sport.

Situation 9
Yanis accepte tous les cookies sur un site sans lire les informations. Plus tard, il constate que des publicités apparaissent sur d'autres sites en lien avec ce qu'il a consulté.

Situation 10
Léa publie un message pour souhaiter un bon anniversaire à son amie en mentionnant son âge et en ajoutant une photo d'elle enfant, sans lui demander son avis.

Pour chaque situation, les élèves peuvent répondre aux questions suivantes :

- Quelles informations sont partagées ?
- Quelles sont les conséquences possibles et pour qui ?
- Est-ce respectueux ?
- Que faudrait-il faire autrement ?

Support 2.3 : Synthèse des bonnes pratiques

Les élèves co-construisent une synthèse des bonnes pratiques, suivie d'un choix individuel de trois actions concrètes à appliquer durant le mois pour renforcer leur protection numérique.

Exemple concret

Les bons réflexes pour protéger son identité numérique

- Je réfléchis avant de publier : ce que je mets en ligne peut être vu par beaucoup de personnes et rester longtemps en ligne
- Je limite les informations personnelles : je ne partage pas mon nom, mon adresse, mon âge, mon numéro de téléphone ou ma localisation
- Je respecte les autres : je demande l'accord avant de publier une photo ou un contenu qui les concerne
- Je vérifie les informations avant de les partager
- Je paramètre la confidentialité de mes comptes pour contrôler qui peut accéder à mes publications ou mes réactions

3 axes d'actions à retenir

1. Se protéger
- Ne pas donner d'informations sensibles
- Faire attention aux applications utilisées et aux règles d'utilisation

2. Réfléchir avant d'agir
- Se demander : « Est-ce que je peux assumer cette publication ? »
- Vérifier les contenus avant de les partager
- Penser aux conséquences pour moi ou pour les autres

3. Respecter les autres
- Ne pas publier sans autorisation
- Éviter les propos blessants

Règles d'or de la vie en ligne

1. Je ne partage pas tout
Je garde mes informations personnelles privées.

2. Je réfléchis avant de publier
Je n'ai pas tous les droits, et Internet garde des traces.

3. Je contrôle qui voit mes contenus
Je vérifie mes paramètres de comptes.

4. Je respecte les autres
Je ne publie rien sans leur accord et je n'écris pas de commentaires blessants.

5. Je lis avant d'accepter
Je lis et réfléchis avant d'accepter d'installer une application, d'accepter les cookies…

3 Gérer sa sécurité numérique
Propositions d'activités

Attendus visés

- **Savoir** : Décoder une signalétique (PEGI…)
- **Savoir** : Distinguer HTTP et HTTPS

Exemples d'activités

Expert en sécurité des contenus numériques

Objectifs : comprendre et utiliser la signalétique (PEGI…) pour faire des choix adaptés et sécurisés.

Déroulement de l'activité

- **Classification de pictogrammes (Support 1.1)**
  Les élèves endossent le rôle d'« experts en classification ». Leur mission : conseiller une plate-forme de divertissement (jeux/films) pour optimiser la protection des mineurs et sécuriser leur identité numérique. Dans un premier temps, ils reçoivent une série de pictogrammes sans explication. Par petits groupes, ils observent les indices visuels (formes, couleurs, symboles, chiffres) et formulent des hypothèses sur leur signification. Ils vérifient ensuite en associant chaque pictogramme à sa définition officielle.
- **Analyse des pictogrammes (Support 1.2)**
  Ensuite, ils analysent des jaquettes de jeux ou films comportant des pictogrammes.
  Leur mission est de décider si ces contenus sont adaptés à un public donné (ex. : 10 ans) en justifiant leur choix à partir des symboles observés.
- **Création d'un nouveau pictogramme (Support 1.3)**
  Pour affiner leur compréhension, les élèves réagissent à des affirmations (vrai ou faux) sur le système PEGI afin de corriger les idées reçues et mieux comprendre le rôle de l'outil. Enfin, les élèves inventent un nouveau pictogramme pour signaler un type de contenu ou de risque (ex. : dépendance, achats intégrés…), qu'ils présentent au reste de la classe.

Sécuriser une connexion Internet

Objectif : distinguer HTTP et HTTPS et adopter des comportements sécurisés lors de la navigation.

Déroulement de l'activité

- **Comparaison entre HTTP et HTTPS (Support 2.1)**
  Les élèves comparent deux types de messages, l'un en clair (HTTP), l'autre codé (HTTPS). Ils constatent rapidement que le message « HTTP » peut être lu et compris facilement, contrairement au message « HTTPS » qui est « codé » ou « chiffré ».
- **Analyse d'adresses de sites (Support 2.2)**
  Les élèves analysent ensuite des adresses de sites afin de trouver un indice de sécurité : la présence de HTTPS en début d'URL. Ils apprennent à lire une URL et à repérer certains éléments essentiels liés à la protection des données.
- **Analyse de situations (Support 2.3)**
  L'activité se poursuit avec l'analyse de situations concrètes (création de comptes, achat en ligne, envoi d'informations…). Les élèves doivent déterminer si chaque situation est sûre ou risquée, et justifier leurs choix.

Ressources

Pour approfondir le sujet ou compléter ces activités avec des exercices, vous trouverez des ressources gratuites sur :
e-classe.be/numerique-s1-securite

Expert en sécurité des contenus numériques

Objectifs : comprendre et utiliser la signalétique (PEGI…) pour faire des choix adaptés et sécurisés.

Support 1.1 : Classification de pictogrammes

Les élèves endossent le rôle d'« experts en classification ». Leur mission : conseiller une plateforme de divertissement (jeux/films) pour optimiser la protection des mineurs et sécuriser leur identité numérique. Dans un premier temps, ils reçoivent une série de pictogrammes sans explication. Par petits groupes, ils observent les indices visuels (formes, couleurs, symboles, chiffres) et formulent des hypothèses sur leur signification. Ils vérifient ensuite en associant chaque pictogramme à sa définition officielle.

Exemple concret

Où trouver les pictogrammes PEGI et leur signification ?

https://pegi.info/fr
https://icons8.com/icons/set/pegi-pegi

Dépassement possible

Introduire des pictogrammes inexistants dans le système officiel PEGI et pousser les élèves à avoir un esprit critique. **Astuce :** pour insérer des pictogrammes dans un document textuel, utiliser la combinaison de touches [Windows] + [.] sur Windows.

Exemples de pictogrammes « réalistes »

- 🔞 Interdit aux moins de 18 ans
- 💳 Contenu payant
- 📱 Contenu interactif
- ⚠️ Avertissement général, danger
- 🍭 Contenu enfantin et ludique
- 🎵 Contenu musical

Exemples de pictogrammes « farfelus »

- 🐍 « Dangereux pour les serpents »
- 👽 « Contenu extraterrestre »
- 🌈 « Contenu multicolore »
- 🍕 « Contenu comestible »
- 🏆 « Contenu compétitif »
- ✈️ « Contenu réservé aux avions »

Support 1.2 : Analyse des pictogrammes

Ensuite, les élèves analysent des jaquettes de jeux ou films comportant des pictogrammes. Leur mission est de décider si ces contenus sont adaptés à un public donné (exemple : 10 ans) en justifiant leur choix à partir des symboles observés.

Exemple concret

www.jeuxactu.com/divers/images-divers-jeux-video-757-4.htm#img
www.cinemapassion.com/jaquette-de-dvd-A.php

Support 1.3 : Création d'un nouveau pictogramme

Pour affiner leur compréhension, les élèves réagissent à des affirmations (vrai/faux) sur le système PEGI afin de corriger les idées reçues et mieux comprendre le rôle de l'outil.

Exemple concret

1. Les symboles PEGI indiquent la difficulté du jeu
Faux. Il indique l'âge minimum recommandé, pas la difficulté.

2. Les symboles PEGI montrent le type de contenu sensible
Vrai. Violence, peur, langage grossier, interactions en ligne, etc.

3. PEGI interdit la vente du produit aux plus jeunes que l'âge indiqué
Faux. Le chiffre est une recommandation, pas une interdiction légale.

4. Le symbole « langage grossier » indique que le jeu contient des mots vulgaires
Vrai. Il alerte sur le contenu verbal inapproprié pour les plus jeunes.

5. Le symbole PEGI 3 indique la présence de scènes de violence réaliste
Faux. Les films ou jeux vidéo labellisés PEGI 3 ne contiennent pas de violence ou alors uniquement des bagarres de dessins animés (non effrayante, pas de sang, des étoiles autour de la tête d'un personnage…)

6. Les pictogrammes PEGI sont identiques dans tous les pays
Faux. Certains pays adaptent légèrement les icônes mais gardent le même sens global.

7. Un jeu PEGI 16 peut contenir du sang ou des combats réalistes
Vrai. PEGI 16 correspond à des contenus plus réalistes et potentiellement sombres ou violents.

8. PEGI évalue également la qualité éducative d'un jeu
Faux. PEGI évalue la sécurité vis-à-vis du contenu, pas la valeur pédagogique.

9. Les parents peuvent se fier aux pictogrammes pour choisir un jeu adapté à leur enfant
Vrai. Les pictogrammes servent de guide fiable pour les âges et contenus.

10. Les symboles PEGI remplacent toutes les autres informations sur le jeu
Faux. Ils complètent d'autres informations (résumé, plateforme, prix…) mais ne remplacent pas tout.

Sécuriser une connexion Internet

Objectif : distinguer HTTP et HTTPS et adopter des comportements sécurisés lors de la navigation.

Support 2.1 : Comparaison entre HTTP et HTTPS

Les élèves comparent deux types de messages, l'un envoyé en clair (HTTP), l'autre codé (HTTPS). Ils constatent rapidement que le message « HTTP » peut être lu et compris facilement, contrairement au message « HTTPS » qui est « codé » ou « chiffré ».

Exemple concret

1. Message simple
HTTP : « Rendez-vous à 15 h dans la cour ! »
HTTPS : « 18.5.14.4.5.26-22.15.21.19-1-(15).8-4.1.14.19-12.1-3.15.21.18(!) »

2. Message avec information personnelle
HTTP : « Mon mot de passe est soleil123 »
HTTPS : «13.15.14-13.15.20-4.5-16.1.19.19.5-5.19.20-19.15.12.5.9.12.(123) »

3. Achat en ligne
HTTP : « Je paie avec la carte 1234567890123456 »
HTTPS : « 10.5-16.1.9.5-1.22.5.3-12.1-3.1.18.20.5-(1234567890123456) »

4. Création de compte
HTTP : « Mon adresse électronique est jeandupont@email.com »
HTTPS : « 13.15.14-5.13.1.9.12-5.19.20-10.5.1.14.4.21.16.15.14.20(@)5.13.1.9.12(.)3.15.13 »

5. Message « secret » entre amis
HTTP : « Le code secret est dragon »
HTTPS : « 12.5-3.15.4.5-19.5.3.18.5.20-5.19.20-4.18.1.7.15.14 »

6. Message scolaire
HTTP : « Le contrôle est reporté à demain. »
HTTPS : « 12.5-3.15.14.20.18.15.12.5-5.19.20-18.5.16.15.18.20.5-1-4.5.13.1.9.14(.) »

Information complémentaire sur le codage utilisé pour l'exemple :

- Chaque lettre est remplacée par un nombre selon sa place dans l'alphabet (A=1, B=2 …)
- Chaque lettre est séparée de la suivante par un point
- Chaque nombre est gardé tel quel mais mis entre parenthèses
- Chaque espace est remplacé par un tiret
- Chaque caractère spécial ou signe de ponctuation est mis entre parenthèses
- Les accents sont supprimés

Support 2.2 : Analyse d'adresses de sites

Les élèves analysent ensuite des adresses de sites afin de trouver un indice de sécurité : la présence de HTTPS en début d'URL. Ils apprennent à lire une URL et à repérer certains éléments essentiels liés à la protection des données.

Exemple concret

- http://www.jeux-gratuits.com
- http://ecole-exemple.be
- http://shopping-pas-cher.net
- https://www.jeux-gratuits.com
- https://www.amazon.com.be
- https://www.facebook.com
- http://banque-en-ligne-secure.com
- https://www.ing.be
- http://reseau-social-amis.com

Support 2.3 : Analyse de situations

L'activité se poursuit avec l'analyse de situations concrètes (création de compte, achat en ligne, envoi d'informations…). Les élèves doivent déterminer si chaque situation est sûre ou risquée, et justifier leurs choix.

Exemple concret

Création de compte sur un site de jeux

Tu veux créer un compte sur **http://www.superjeux-gratuit.com**.
La page demande la création d'un compte (adresse électronique et mot de passe).

Constats :

- **Le « S » manquant (et l'absence de cadenas 🔒) :** contrairement au site précédent, celui-ci utilise le protocole HTTP (sans le « S » de Secure). Cela signifie que les informations circulent en « clair » sur le réseau. N'importe qui peut intercepter ton adresse électronique et ton mot de passe.
- **Le piège du mot de passe :** si l'utilisateur utilise le même mot de passe que pour sa messagerie électronique ou ses réseaux sociaux (ce que font beaucoup d'élèves), le site (ou un pirate) peut alors accéder à tous ses autres comptes.
- **La fiabilité du site :** un site qui ne sécurise même pas sa page d'inscription est soit très amateur, soit malveillant. C'est souvent une porte d'entrée pour les spams ou les virus.

Le bon réflexe d'expert : ne saisis jamais de données personnelles ou de mots de passe sur un site qui n'affiche pas le HTTPS et le petit cadenas. Et surtout : utilise toujours un mot de passe unique pour chaque nouveau site !

Achat en ligne

Tu achètes un t-shirt sur **https://www.sportstyle.com**.
Un cadenas 🔒 apparaît dans la barre d'adresse juste devant l'url. Le site est connu.
Le site demande une adresse et un numéro de carte bancaire.

Constats

- **La présence d'une double sécurité :** le HTTPS (le « S » et le cadenas) garantit ici que tes coordonnées bancaires sont cryptées pendant l'envoi. Personne ne peut les « intercepter » en chemin.
- **La réputation :** puisque le site est connu, le risque que ce soit une arnaque (phishing) est faible.
- **Attention à la collecte :** si le paiement est sécurisé, n'oublie pas qu'en donnant ton adresse et tes goûts (achat d'un t-shirt de sport), tu fournis des données volontaires. Le site va s'en servir pour t'envoyer des publicités ciblées ou profiler tes habitudes de consommation.

Le bon réflexe d'expert : le cadenas prouve que la « porte » est fermée à clé, pas que le destinataire est ton ami. Même sur un site sûr, coche uniquement les cases obligatoires et refuse l'enregistrement de ta carte bancaire pour plus de sécurité !

Réseau Wi-Fi public

Tu es connecté à un Wi-Fi gratuit dans un lieu public.
Tu veux te connecter à **https://www.moncompte.be** pour vérifier des informations personnelles sur ton compte (adresse enregistrée, date de naissance…).

Conseil
Utiliser le HTTPS sur un Wi-Fi public, c'est comme transporter un coffre-fort dans une rue malfamée. Le contenu est protégé, mais tout le monde voit que tu transportes quelque chose de précieux, sait d'où tu viens, et quelqu'un pourrait essayer de t'arracher le coffre ou de te donner une fausse clé pour l'ouvrir.

Le bon réflexe d'expert : pour des données sensibles, on coupe le Wi-Fi et on utilise la 4G/5G (qui est un tunnel privé et crypté par l'opérateur).

Formulaire en ligne pour un concours

Ce site propose de gagner un smartphone : **http://superarnaque.net**.
Le site demande un nom, un prénom, une adresse et un numéro de téléphone.

Constats

- **Le protocole non sécurisé :** le site est en HTTP (pas de cadenas 🔒). Tes données circulent « en clair » et peuvent être volées par n'importe qui.
- **Le prix des données :** sur Internet, quand c'est gratuit, c'est souvent toi le produit. Ce site n'a probablement pas de smartphone à offrir. Son seul but est de récolter des bases de données de personnes réelles et actives.
- **Conséquences réelles :** une fois tes données fournies, tu t'exposes à du harcèlement téléphonique (spams), à des arnaques par SMS (smishing) ou à la revente de tes informations à des entreprises peu scrupuleuses. Ton identité numérique est désormais « marquée » comme une cible facile.

Le bon réflexe d'expert : si une offre semble trop belle pour être vraie, c'est que c'est une arnaque. Ne donne jamais tes coordonnées personnelles à un site inconnu, surtout pour un gain « facile ».

Partage de fichier

Un ami t'envoie un lien de partage vers le site **https://drive-partage-securise-fichier.org**.
Le site demande de se connecter avec une adresse électronique pour voir le document partagé.

Constats

- **L'usurpation d'identité :** ce n'est peut-être pas ton ami qui t'a envoyé ce message, mais un pirate qui a pris le contrôle de son compte.
- **Le faux site (Typosquattage) :** l'adresse ressemble à un service connu (comme Google Drive), mais l'extension .org et le nom à rallonge sont suspects. Le but est de voler tes identifiants de connexion.
- **Le HTTPS trompeur :** le cadenas 🔒 signifie seulement que la connexion est chiffrée, pas que le propriétaire du site est honnête. Un pirate peut très facilement obtenir un cadenas pour son site frauduleux.

Le bon réflexe d'expert : ne saisis jamais tes identifiants sur un site vers lequel on t'a redirigé par un lien. En cas de doute, contacte ton ami par un autre moyen (SMS, appel) pour vérifier s'il est bien l'auteur de l'envoi.

4 Réagir face à la cyberviolence
Propositions d'activités

Attendus visés

- **Compétence** : Réagir, de manière responsable, face aux risques de cyberattaque, de cyberharcèlement, de cyberdépendance
- **Savoir** : Identifier les moyens de signaler ou bloquer un contenu partagé de manière inappropriée en ligne
- **Savoir-faire** : Proposer et mettre en place des actions pertinentes pour faire face à des situations de cyberattaque, de cyberharcèlement, de cybermanipulation

Exemples d'activités

Enquête numérique – Comprendre et décider

Objectifs : identifier les situations de cyberviolence, analyser les contenus en ligne et déterminer les réactions appropriées.

Déroulement de l'activité

- **Analyse de situations** (Support 1.1)
  Les élèves reçoivent une série de publications (messages, images, commentaires, articles). En groupe, ils analysent chaque situation afin de déterminer s'il s'agit de cyberviolence ou non. Ils s'appuient sur des critères donnés. L'enseignante/l'enseignant relance la réflexion ou la discussion avec les questions proposées pour chaque situation. Les élèves explicitent ensemble les conséquences probables du cyberharcèlement et proposent des réactions possibles : ignorer, répondre, bloquer, signaler, demander de l'aide…
- **Classement des actions à mener** (Support 1.2)
  Les élèves ordonnent les actions suivantes de la plus immédiate à la plus radicale pour mettre fin à la cyberviolence (exemples : faire une capture d'écran, bloquer une personne, signaler un message…).
- **Repèrage des outils de signalement** (Support 1.3)
  À partir d'exemples (captures d'écran) ou de plateformes connues et utilisées en classe, les élèves repèrent les outils de signalement et expliquent leur rôle.

Agir et s'engager – Protéger et soutenir

Objectif : adopter des comportements responsables face à la cyberviolence et développer une posture citoyenne et empathique.

Déroulement de l'activité

- **Réflexions sur les réactions à adopter (Support 2.1)**
  À partir de situations de cyberharcèlement, les élèves réfléchissent aux bonnes réactions à adopter : que faire, à qui en parler, comment protéger la victime.
- **Réflexion sur les actes de prévention (Support 2.2)**
  Les élèves réfléchissent ensuite au rôle des témoins et proposent des pistes ou identifient des responsabilités dans la prévention et l'action face à la cyberviolence.
- **Rédaction d'un message de soutien (Support 2.3)**
  Les élèves rédigent un message de soutien destiné à une victime fictive, en travaillant l'empathie, le respect et les formulations aidantes.
- **Réalisation d'un guide (Support 2.4)**
  Enfin, les élèves réalisent une production concrète : un guide de signalement et de réaction (affiche, fiche ou support numérique). Ce guide reprend les étapes clés, les outils (signaler, bloquer), les bons réflexes et les ressources d'aide.

Ressources

Pour approfondir le sujet ou compléter ces activités avec des exercices, vous trouverez des ressources gratuites sur :
e-classe.be/numerique-s1-securite

Enquête numérique – Comprendre et décider

Objectifs : identifier les situations de cyberviolence, analyser les contenus en ligne et déterminer les réactions appropriées.

Support 1.1 : Analyse de situations

Les élèves reçoivent une série de publications (messages, images, commentaires, articles). En groupe, ils analysent chaque situation afin de déterminer s'il s'agit de cyberviolence ou non. Ils s'appuient sur des critères donnés. L'enseignante/l'enseignant relance la réflexion ou discussion avec les questions proposées pour chaque situation. Les élèves explicitent ensemble les conséquences probables du cyberharcèlement et proposent des réactions possibles : ignorer, répondre, bloquer, signaler, demander de l'aide…

Exemple concret

Critères pour déterminer si le message traduit un conflit ou un harcèlement

1. Message humiliant portant atteinte à la personne
2. Message visible par tous et toutes
3. Message répétitif

Publications fictives

Commentaire sous une publication dans un groupe : « Franchement, t'aurais pu éviter de poster ça… 😒 »	Message dans un groupe privé : « On fait une sortie samedi mais surtout on n'invite pas Alex hein 🤐 »	Message général dans un groupe privé : « Ok les gars ! J'ai chopé le numéro de Sofia ! Appelez-la au 0789 12 34 56 ! »
Messages envoyés à une seule personne, en privé : « T'es vraiment nul 😂 » « Sérieux, t'es nul » « Tout le monde le pense »	Message sous un faux profil appelé *Julio_officiel* : « J'ai raté mon contrôle parce que je suis bête 😜 »	Publication d'une image modifiée d'un élève représenté avec une tête déformée accompagnée du commentaire : « Nouvelle espèce découverte 👽😂 »
Publication d'une photo d'un élève en train de manger avec le commentaire : « Le roi des bouffons 🌭🐷😂 »	Message destiné à une personne précise dans un groupe de classe : « Continue comme ça et tu vas avoir des problèmes demain. »	Message envoyé en privé : « Trop bien ta présentation 👍 »

Questions pour aider l'analyse

Critères simples, accessibles rapidement aux élèves :

- Est -ce que la situation arrive plusieurs fois (suite de messages, répétition…) ?
- Est-ce que le message est méchant, humiliant ou moqueur ?
- Est-ce volontairement visible par beaucoup de personnes ?
- Est-ce que la personne visée peut se sentir blessée, triste ou humiliée ?

Critères intermédiaires, pour une analyse plus fine :

- Plusieurs personnes participent-elles (effet de groupe) ?
- Est-ce que la situation présente une illégalité (droit à l'image, donnée personnelle…) ?
- Le message semble-t-il « humoristique » mais vise en réalité à blesser ?
- Cela peut-il nuire durablement à l'image de la personne ?
- La victime peut-elle « répondre » ou « se défendre » facilement ou est-elle bloquée, voire isolée ?

Support 1.2 : Classement des actions à mener

Les élèves ordonnent les actions suivantes de la plus immédiate à la plus radicale pour mettre fin à la cyberviolence (exemples : faire une capture d'écran, bloquer une personne, signaler un message…).

Exemple concret

1. Observer / analyser
- Lire attentivement le message ou la publication
- Vérifier si c'est une blague, un conflit ou une attaque
- Regarder si d'autres messages similaires existent
- Identifier si d'autres personnes participent

2. Garder des preuves
- Faire une capture d'écran
- Enregistrer les messages
- Noter la date et l'heure

3. Se protéger immédiatement
- Ne pas répondre sous le coup de la colère
- Bloquer la personne
- Mettre son compte en privé

4. Agir sur la plateforme
- Signaler le contenu
- Signaler le compte si besoin

5. Demander de l'aide
- En parler à un adulte de confiance
- Contacter un service d'aide
- En parler à un ami ou une amie de confiance

6. Soutenir la victime (si témoin)
- Soutenir la victime
- Signaler le contenu en tant que témoin
- Ne pas relayer ou liker le contenu

Propositions d'actions à discuter pour faire réfléchir les élèves
- Répondre avec une insulte
- Se venger en publiant à son tour
- Partager la publication « pour montrer aux autres »
- Ignorer systématiquement même si c'est grave
- Supprimer sans garder de preuve

Support 1.3 : Repèrage des outils de signalement

À partir d'exemples (captures d'écran) ou de plateformes connues et utilisées en classe, les élèves repèrent les outils de signalement et expliquent leur rôle.

Exemple concret

Le bouton « **Signaler** » permet de signaler un message, une photo/vidéo, un commentaire, un compte. Il est souvent représenté par un point d'exclamation (!), un drapeau (🚩) ou dans un menu d'options.

Bloquer un utilisateur ou une utilisatrice peut parfois permettre de se protéger directement. Cela empêche la personne de continuer à voir le profil, d'envoyer des messages, de commenter… C'est une première action de protection, mais elle ne remplace pas le signalement.

Si on est propriétaire du contenu, et après avoir gardé une preuve (capture d'écran par exemple), il peut être utile de **supprimer un contenu** (commentaire reçu ou publication qui est à l'origine de problèmes).

Paramétrer les options de confidentialité peut permettre de prévenir certaines situations. Par exemple, mettre son compte en « privé », limiter qui peut commenter, envoyer des messages, voir les publications…

Signaler le(s) problème(s) à un adulte de confiance ou à l'école est essentiel pour que la situation soit connue et traitée !

Il existe également des **services spécialisés** qui peuvent intervenir ou accompagner. Le premier contact sera généralement le centre PMS.

Agir et s'engager – Protéger et soutenir

Objectif : adopter des comportements responsables face à la cyberviolence et développer une posture citoyenne et empathique.

Support 2.1 : Réflexions sur les réactions à adopter

À partir de situations de cyberharcèlement, les élèves réfléchissent aux bonnes réactions à adopter : que faire, à qui en parler, comment protéger la victime. Ils confrontent leurs idées et construisent une synthèse des bonnes pratiques en lien avec la charte de l'école.

Exemple concret

Situation 1
Un/une élève reçoit chaque soir des messages privés contenant des moqueries sur son apparence. Plusieurs élèves participent à ces envois.

Situation 2
Une conversation de classe est créée sans un/une élève. Dans ce groupe, les autres se moquent régulièrement de lui/elle et partagent des captures de ses publications.

Situation 3
Une photo embarrassante prise à l'école est publiée sur un réseau social sans l'accord de l'élève concerné, accompagnée de commentaires humiliants.

Situation 4
Quelqu'un crée un faux profil au nom d'un/une élève et publie des messages ridicules ou insultants pour se moquer de lui/elle.

Situation 5
Sous une publication (photo, vidéo), plusieurs élèves laissent des commentaires négatifs, moqueurs ou insultants, visibles par tout le monde.

Situation 6
Lors d'un jeu en ligne, un joueur/une joueuse est constamment insulté par d'autres joueurs qui se liguent contre lui/elle et l'excluent volontairement.

Situation 7
Une fausse information circule sur un/une élève. Elle est relayée et amplifiée par plusieurs personnes sur différents réseaux.

Situation 8
Un/une élève reçoit des messages privés contenant des menaces (« tu vas le regretter », « fais attention demain »…)

Situation 9
Un groupe insiste pour qu'un/une élève envoie une photo personnelle. Après refus, il/elle est insulté et ridiculisé publiquement.

Situation 10
Une image ou vidéo est modifiée (montage) pour ridiculiser un/une élève, puis partagée largement dans la classe ou sur les réseaux.

Support 2.2 : Classement des actions à mener

Les élèves réfléchissent ensuite au rôle des témoins et proposent des pistes ou identifient des responsabilités dans la prévention et l'action face à la cyberviolence.

Exemple concret

Actions problématiques

- Rire ou liker les contenus, c'est encourager l'agresseur et banaliser la violence
- Partager ou relayer la publication, c'est amplifier la diffusion et aggraver le harcèlement
- Ne rien faire (passivité), c'est laisser la victime seule et donner l'impression que c'est « normal »
- Participer indirectement (commentaires ambigus), c'est renforcer le groupe contre la victime

Postures positives de témoins

1. Le témoin protecteur tente de limiter la propagation :

- Il refuse de relayer le contenu
- Il signale la publication (réseaux sociaux, plateforme)
- Il encourage les autres à arrêter

2. Le témoin soutenant tente de soutenir psychologiquement la victime :

- Il envoie un message privé à la victime
- Il lui dit qu'elle n'est pas seule
- Il valorise la personne

3. Le témoin alerteur tente de faire intervenir quelqu'un qui peut agir :

- Il prévient un adulte de confiance (enseignant/enseignante, éducateur/éducatrice, parent)
- Il peut accompagner la victime pour en parler

4. Le témoin engagé tente de faire évoluer les normes du groupe :

- Il intervient publiquement (sans agresser)
- Il rappelle les règles :
  › « Ce n'est pas drôle »
  › « Ça peut faire du mal »

5. Le témoin médiateur apaise la situation :

- Il tente de désamorcer calmement
- Il évite l'escalade

Support 2.3 : Rédaction d'un message de soutien

Les élèves rédigent un message de soutien destiné à une victime fictive, en travaillant l'empathie, le respect et les formulations aidantes.

Exemple concret

- « Je viens de voir ce qui se passe, et je suis vraiment désolé(e) pour toi. »
- « Ce qu'ils disent est injuste. Ne les laisse pas te faire douter de ta valeur. »
- « Ça doit être très difficile à vivre… Si tu veux, on peut en parler ensemble. »
- « Je comprends que ça puisse te faire du mal. »
- « Ne laisse pas ces messages définir qui tu es. Tu es quelqu'un de bien. »
- « Ceux qui font ça cherchent à blesser, mais ça ne dit rien de toi. »
- « Tu peux en parler à un adulte. Je peux t'accompagner si tu veux. »
- « Tu n'es pas seul/seule. Si tu veux en parler, je suis là pour toi. »
- « On peut signaler ça ensemble si tu veux. »

Où répondre ?

Le choix du canal pour exprimer son soutien — privé ou public — modifie radicalement la portée de l'acte. Si un message privé sécurise la relation entre l'allié/l'alliée et la victime, une intervention sur un groupe public engage toute la communauté. Cette dernière peut alors s'unir contre l'agresseur/l'agresseuse, mais au risque de renverser le harcèlement ou d'enfermer l'intervenant/l'intervenante dans un rôle complexe de « sauveur/sauveuse » ou de nouvelle cible. L'objectif n'est pas de définir une réponse idéale, mais d'amener les élèves à conscientiser ces dynamiques sociales pour agir de manière éclairée.

Support 2.4 : Réalisation d'un guide

Enfin, les élèves réalisent une production concrète : un guide de signalement et de réaction (affiche, fiche ou support numérique). Ce guide reprend les étapes clés, les outils (signaler, bloquer), les bons réflexes et les ressources d'aide.

Exemple concret

- **Une boite à outils pour lutter contre le cyberharcèlement :**
  https://prof.cfwb.be/article/une-boite-a-outils-pour-lutter-contre-le-harcelement
- **Un court métrage contre le cyberharcèlement :**
  https://www.youtube.com/watch?v=-oDL3brtoz8
- **Harcèlement à l'école : les 3 rôles qu'il faut connaître – HOPE :**
  https://www.youtube.com/watch?v=uc_f7tpr1U8
- **Le cyberharcèlement vu par des élèves du secondaire :**
  https://instructionpublique.bruxelles.be/fr/actualites/le-cyberharcelement-vu-par-des-eleves-de-linstitut-diderot

5 Gérer son bien-être numérique
Propositions d'activités

Attendus visés

- **Compétence** : Réagir, de manière responsable, face aux risques de cyberattaque, de cyberharcèlement, de cyberdépendance
- **Savoir** : Citer des situations où il est préférable de demander de l'aide humaine plutôt que de se tourner vers l'IA pour son bien-être numérique, psychologique et social
- **Savoir** : Citer des méthodes utilisées par des plateformes en ligne ou des réseaux sociaux pour « capturer » l'attention des utilisateurs
- **Savoir** : Citer des avantages du droit à la déconnexion, tant pour soi-même que pour les autres
- **Savoir-faire** : Repérer ses habitudes numériques et expliquer en quoi cette analyse peut améliorer son organisation de temps et son bien-être

Exemples d'activités

Es-tu maitre de ton écran… ou est-ce lui qui te contrôle ?

Objectifs : amener les élèves à analyser leurs habitudes numériques, comprendre les mécanismes qui captent leur attention et prendre conscience des bénéfices du droit à la déconnexion afin d'améliorer leur bien-être.

Déroulement de l'activité :

- **Phase d'introspection (Support 1.1)**
  Les élèves estiment leur temps d'écran quotidien et identifient leurs usages principaux (réseaux sociaux, jeux, vidéos, communication). Ils complètent un tableau et comparent leurs estimations avec les données réelles issues de leurs appareils. Cette première étape permet de faire prendre conscience des habitudes.
- **Analyse des outils (Support 1.2)**
  Dans un second temps, les élèves travaillent en petits groupes à l'analyse de techniques qui poussent les utilisateurs à rester en ligne. Ils analysent les outils qu'ils utilisent afin de déterminer si ces techniques les influencent.
- **Débat dynamique (Support 1.3 - 1.4)**
  L'enseignante/l'enseignant propose ensuite un débat dynamique en soumettant des affirmations telles que « Il faut toujours répondre immédiatement aux messages » ou « Être connecté en permanence est indispensable ». Les élèves se positionnent physiquement dans la classe et justifient leur point de vue. Cette discussion met en évidence les avantages du droit à la déconnexion : amélioration du sommeil, de la concentration, réduction du stress et meilleure qualité des relations sociales…

- **Analyse des contenus (Support 1.5)**
  Les élèves analysent des exemples de contenus en ligne conçus pour attirer ou manipuler (titres sensationnalistes, images trompeuses, messages émotionnels). Ils identifient les stratégies utilisées pour capter leur attention et influencer leurs réactions. Ils font des liens avec leur propre expérience numérique et renforcent leur esprit critique face aux contenus en ligne.

IA ou humain : à qui faire confiance quand ça compte vraiment ?

Objectifs : aider les élèves à identifier les limites de l'intelligence artificielle (IA), reconnaître les situations où l'aide humaine est essentielle et développer un esprit critique face aux contenus et aux systèmes numériques.

Déroulement de l'activité :

- **Échanges sur l'IA (Support 2.1)**
  Face à des situations du quotidien numérique et personnel, les élèves décident s'il est préférable de faire appel à une intelligence artificielle ou à un être humain et doivent justifier leur choix. Les échanges mènent à la distinction claire des situations où l'IA peut être utile (recherche d'informations, aide à l'organisation…) de celles qui nécessitent une intervention humaine (gestion des émotions, conflits, cyberharcèlement, situations complexes…).
  Cette première étape met en évidence l'importance de l'empathie, du jugement et de l'accompagnement humain.
- **Carte mentale des aides disponibles (Support 2.2)**
  Ensuite, les élèves identifient les personnes et ressources vers lesquelles ils peuvent se tourner en cas d e difficulté. Ils construisent une carte mentale ou un tableau en classant ces aides selon différents types de besoins : techniques, émotionnels, relationnels… Cette étape vise à renforcer le réflexe de demander de l'aide et à rendre ces ressources concrètes et accessibles.

Ressources

Pour approfondir le sujet ou compléter ces activités avec des exercices, vous trouverez des ressources gratuites sur :
e-classe.be/numerique-s1-securite

Es-tu maitre de ton écran… ou est-ce lui qui te contrôle ?

Objectifs : amener les élèves à analyser leurs habitudes numériques, comprendre les mécanismes qui captent leur attention et prendre conscience des bénéfices du droit à la déconnexion afin d'améliorer leur bien-être.

Support 1.1 : Phase d'introspection

Lors d'une phase d'introspection, les élèves estiment leur temps d'écran quotidien et identifient leurs usages principaux (réseaux sociaux, jeux, vidéos, communication). Ils complètent un tableau et comparent leurs estimations avec les données réelles issues de leurs appareils. Cette première étape permet de faire prendre conscience des habitudes.

Exemple concret

Estimation des usages

Activité numérique	Temps estimés par jour	Moment de la journée	Pourquoi je l'utilise ?	Seul ou avec d'autres ?
Réseaux sociaux				
Jeux vidéo				
Streaming				
Messagerie				
Autres				

Données réelles disponibles sur les appareils

Activité – Application	Temps réel mesuré	Écart avec mon estimation (+ / -)	Est-ce une surprise ? (oui/non)

Support 1.2 : Analyse des outils

Dans un second temps, les élèves travaillent en petits groupes à l'analyse de techniques qui poussent les utilisateurs et utilisatrices à rester en ligne. Ils analysent les outils qu'ils utilisent afin de déterminer si ces techniques les influencent.

Exemple concret

Éléments qui attirent l'attention et incitent à rester connecté :

- Scroll infini – défilement sans fin
- Notifications
- Récompenses (likes, scores, badges)
- Lecture automatique des médias (vidéo, audio)
- Contenus courts (shorts, réels, stories…) qui s'enchainent
- Contenus éphémères « qu'on ne veut donc pas louper »
- Recommandations personnalisées et automatiques
- Indicateur de présence (présence en ligne, en train d'écrire…)
- Couleurs vives et « flash »

Analyser les outils utilisés par la classe, à l'école ou en dehors. Déterminer si certaines méthodes sont reconnues dans les outils et détailler leur impact sur le comportement des élèves.

Quelques pistes pour guider les réflexions

Les outils et plateformes jouent sur…

- La curiosité
- Le besoin de reconnaissance
- La peur de manquer un message ou une notification
- Le plaisir du jeu ou de la récompense
- Les habitudes automatiques

Support 1.3 : Débat dynamique

L'enseignant/l'enseignante propose ensuite un débat dynamique en soumettant des affirmations telles que « Il faut toujours répondre immédiatement aux messages » ou « Être connecté en permanence est indispensable ».

Exemple concret

- Il faut toujours répondre immédiatement aux messages
- Être connecté en permanence est indispensable aujourd'hui
- Les notifications sont utiles et ne dérangent pas la concentration
- Passer beaucoup de temps sur les réseaux sociaux est normal
- On peut facilement contrôler son temps d'écran sans aide
- Les applications sont conçues pour nous faire rester le plus longtemps possible
- Ne pas répondre rapidement peut nuire aux relations sociales
- Les écrans empêchent de bien dormir
- Regarder des vidéos ou jouer est un bon moyen de se détendre
- Les jeunes savent mieux gérer leur usage du numérique que les adultes
- Se déconnecter permet de profiter davantage du moment présent

Support 1.4 : Débat dynamique

Les élèves se positionnent physiquement dans la classe et justifient leur point de vue.
Cette discussion met en évidence les avantages du droit à la déconnexion : amélioration du sommeil, de la concentration, réduction du stress et meilleure qualité des relations sociales…

Exemple concret

Avantages du droit à la déconnexion

- Amélioration du sommeil : moins d'exposition aux écrans avant de dormir
- Meilleure concentration : réduction des distractions et des interruptions
- Diminution du stress : moins de pression liée aux notifications et aux réponses immédiates
- Bien-être mental : recul face aux réseaux sociaux et à la comparaison sociale
- Relations sociales de meilleure qualité : interactions plus authentiques en face à face
- Meilleure gestion du temps : plus de place pour d'autres activités (sport, loisirs, repos)
- Autonomie et contrôle : sentiment de maîtriser ses usages numériques

Difficultés potentielles liées à la déconnexion

- Sentiment d'exclusion ou de « rater quelque chose »
- Difficulté à décrocher : habitudes très ancrées
- Pression sociale : attentes des autres (réponses rapides, disponibilité constante)
- Isolement possible : moins de contacts en ligne si la déconnexion est trop stricte
- Organisation à adapter : nécessité de prévenir ou de planifier autrement ses échanges

Support 1.5 : Analyse des contenus

Les élèves analysent des exemples de contenus en ligne conçus pour attirer ou manipuler (titres sensationnalistes, images trompeuses, messages émotionnels). Ils identifient les stratégies utilisées pour capter leur attention et influencer leurs réactions. Ils font des liens avec leur propre expérience numérique et renforcent leur esprit critique face aux contenus en ligne.

Exemple concret

Contenu 1
« 🔥 Tu ne devineras JAMAIS ce qui s'est passé dans cette école… Regarde jusqu'à la fin 😱 »

Technique : piège-à-clics + éveil de la curiosité sans la moindre information valable
Problème : manipulation de l'attention

Contenu 2
« ⚠️ Ton compte sera supprimé dans 24 h ! Clique ici pour le sécuriser. »

Technique : sentiment d'urgence (infondé) + utilisation de la peur
Problème : risque d'action sans réflexion, sans vérification du contexte ou des informations

Contenu 3
« 💸 Gagne 500 € par jour sans effort ! Inscris-toi maintenant. »

Technique : promesse de récompense, de cadeau « facile » ou de promo
Problème : promesse irréaliste ; appât pour une arnaque ou la collecte de données

Contenu 4
« 🚫 Cet aliment est interdit dans plusieurs pays… et pourtant vendu ici ! »

Technique : utilisation de la peur + très souvent de la désinformation basée sur de fausses sources et des « pseudo-spécialistes » bidons
Problème : risque de propagation de fausses informations, de manipulation des gens ou de leur opinion sur un sujet

Contenu 5
« Salut 😊 Clique ici pour voir mes photos privées 👉 [lien] »

Technique : manipulation car « message crédible » ou une mise en confiance + lien suspect (URL manipulé ou trompeur)
Problème : risque de clic sur le lien pouvant renvoyer vers un site dangereux ou déclencher une action dangereuse (vol de données, implémentation d'un virus…)

Contenu 6
« Si tu ne partages pas cette vidéo, c'est que tu n'as pas de cœur 💔 »

Technique : culpabilisation ; photo ou visuel trompeur, voire faux
Problème : pression sociale infondée et risque d'action contraire à son avis propre

Contenu 7
« 🔥 Tu as une série de 7 jours ! Connecte-toi pour ne pas la perdre ! »

Technique : création d'une envie, voire d'une addiction, de l'attente d'une récompense, d'une illusion de perte
Problème : monopolisation de l'attention, génération d'une contrainte ou d'une peur de « perdre » quelque chose

Contenu 8
« Avec cette IA, j'ai réussi tous mes examens sans travailler 😜 »

Technique : promesse de résultat ou d'une « récompense » sans effort ; personnification de l'action (on croit que quelqu'un l'a déjà fait) pour la rendre plus crédible
Problème : information difficile (voire impossible) à vérifier ; propagation de comportements problématiques ou inadaptés

IA ou humain : à qui faire confiance quand ça compte vraiment ?

Objectifs : aider les élèves à identifier les limites de l'intelligence artificielle (IA), reconnaître les situations où l'aide humaine est essentielle et développer un esprit critique face aux contenus et aux systèmes numériques.

Support 2.1 : Échanges sur l'IA

Face à des situations du quotidien numérique et personnel, les élèves décident s'il est préférable de faire appel à une intelligence artificielle ou à un être humain, et doivent justifier leur choix. Les échanges mènent à la distinction claire des situations où l'IA peut être utile (recherche d'informations, aide à l'organisation…) de celles qui nécessitent une intervention humaine (gestion des émotions, conflits, cyberharcèlement, situations complexes…). Cette première étape met en évidence l'importance de l'empathie, du jugement et de l'accompagnement humain.

Exemple concret

- Tu te sens stressé(e) avant un contrôle important
- Tu reçois un message insultant dans un groupe de discussion
- Tu ne comprends pas un exercice de math
- Un camarade publie une photo de toi sans ton autorisation
- Tu cherches des idées pour organiser ton travail scolaire
- Tu te sens triste sans vraiment savoir pourquoi
- Tu as un conflit avec un ami/une amie à cause d'un message mal interprété
- Tu veux améliorer ton sommeil et réduire les écrans le soir
- Tu reçois un message d'un inconnu/une inconnue qui te met mal à l'aise
- Tu as l'impression d'être dépendant(e) aux réseaux sociaux
- Tu dois résoudre un problème technique sur ton ordinateur
- Tu vois une vidéo choquante circuler en ligne
- Tu veux apprendre à mieux configurer ton téléphone
- Tu hésites à partager une information personnelle en ligne

Support 2.2 : Analyse des contenus

Ensuite, les élèves identifient les personnes et ressources vers lesquelles ils peuvent se tourner en cas de difficulté. Ils construisent une carte mentale ou un tableau en classant ces aides selon différents types de besoins : techniques, émotionnels, relationnels… Cette étape vise à renforcer le réflexe de demander de l'aide et à rendre ces ressources concrètes et accessibles.

Exemple concret

Entourage proche
- Parents ou responsables légaux
- Frères et sœurs
- Membres de la famille (grands-parents, oncles, tantes…)
- Amis de confiance

À l'école
- Enseignante et enseignant
- Éducatrice et éducateur
- Directrice et directeur
- Médiatrice et médiateur scolaire
- Psychologue du CPMS

Professionnels et aides extérieures
- Psychologue
- Médecin généraliste
- Assistante ou assistant social
- Éducatrice ou éducateur spécialisé

Services d'aide et d'écoute (Belgique)
- Écoute-enfants (numéro 103)
- Child Focus (116 000 ou signalement en ligne)
- Télé-accueil (107)

Le saviez-vous ?

Les enseignantes et enseignants peuvent s'exercer aux compétences numériques abordées dans ce recueil grâce à des parcours Pix mis à la leur disposition par la Fédération Wallonie-Bruxelles et conçus en collaboration avec l'IFPC. D'autres parcours, adaptés aux élèves, sont également disponibles.

Rendez-vous sur cette ressource pour découvrir les parcours en lien avec le FMTTN : **e-classe.be/pix-fmttn-numerique**

N.B. L'utilisation de parcours Pix avec les élèves nécessite l'acquisition d'une plateforme Pix Orga. Pour tout renseignement : **e-classe.be/pix-orga-enseignement**

Retrouvez cette ressource et de nombreuses autres sur **e-classe.be**

Ressources spécifiques pour le tronc commun : **e-classe.be/ressources-tronc-commun**

Note : les ressources du tronc commun (fiches-info, fiches-outils, recueils d'activités) sont destinés à outiller les enseignants et les enseignantes, en proposant des pistes d'activités et/ou théoriques pour aborder certains attendus des référentiels du tronc commun, dans le respect de la liberté pédagogique.

En ce sens, elles consistent bien en des propositions faites à la communauté éducative et ne sont en aucun cas obligatoires. Pour contribuer à un apprentissage structurel et installé, ces documents doivent s'intégrer à une situation d'apprentissage plus large et plus complexe que l'enseignante/l'enseignant construit, puis met en place avec ses élèves.

Fédération Wallonie-Bruxelles / Ministère • www.fw-b.be
02 413 3000 (les jours ouvrables, de 8h30 à 17h)

Administration générale de l'Enseignement
Service général du Numérique éducatif
Avenue du port 16, 1080 Bruxelles
contact.sgne@cfwb.be

www.enseignement.be

Rédaction : Anne Belien, Frédéric Ernalsteen, Anne Leclercq, Sophie Petyt, Cédric Van Damme, Elisa Tomsin, Claude Van Opstal
Graphisme : Laura Maugeri

Éditeur responsable : Fabrice Aerts-Bancken, Administrateur général a.i. • Avenue du Port 16, 1080 Bruxelles