MON CAHIER DE FORMATION NUMÉRIQUE

Responsabilité, Vie Privée et Sécurité en Ligne

Formation numérique ▪ 1re année du tronc commun (S1) ▪ septembre 2026 ▪ version 0.2

Dans ce cahier, tu vas découvrir tes droits et tes responsabilités sur Internet, apprendre à mieux connaître tes habitudes numériques, et repérer les pièges et les arnaques en ligne.

SCIENCE INFUSE

UCLouvain

Séance 1 — Les droits et les responsabilités sur Internet

TEMPS 1.1 — Découverte du droit d'auteur

Observe la bande dessinée ci-dessous.

Réponds à ces questions.

Que raconte cette histoire ?

Selon toi, quel droit est mis en cause ici ?

TEMPS 1.2 — Création d'une bande dessinée par groupe

En groupe, tu vas recevoir un droit numérique différent. Complète le cadre ci-dessous pour préparer ta bande dessinée.

Groupe n° : .....

Droit attribué : .....

*Attention : ne nomme **pas** le droit dans ta BD. Les autres groupes doivent pouvoir le deviner.*

Ta mission

Invente une histoire en **3 à 9 cases** qui illustre une situation où ce droit est **respecté** ou **violé**.

- Prépare un scénario : décris chaque case et chaque bulle sur une feuille de brouillon.
- Maximum **2 personnages** visibles (d'autres peuvent exister hors-champ)
- On doit comprendre : **la situation** → **le problème** → **la bonne attitude**
- Fais d'abord un croquis dans ces cases

Ta bande dessinée

i Et après ?

Une fois ton croquis terminé, tu peux l'améliorer à la main (dessin soigné, couleurs…) ou réaliser une version numérique avec BDnF (bdnf.bnf.fr) ou Canva.

TEMPS 1.3 — Échange et devinette entre groupes

Chaque groupe présente sa BD sans nommer le droit illustré. À toi de deviner quel droit est représenté dans les BD des autres groupes, puis de compléter le tableau ci-dessous.

Numéro de groupe	Résumé de l'histoire	Droit illustré	Avantage(s) de ce droit
0	Jules s'approprie une œuvre d'un artiste en la publiant sur Instagram sans en mentionner l'auteur.	Droit d'auteur	Personne ne peut voler ton travail ; tu es reconnu comme le vrai créateur ou la vraie créatrice.

★ À RETENIR — LES DROITS NUMÉRIQUES

- **Droit d'auteur :** Ce droit protège les créateurs (musiciens, artistes, écrivains) en interdisant l'utilisation de leurs œuvres sans leur permission.
- **Droit à la vie privée :** Ce droit protège ta vie personnelle : personne ne peut publier des informations ou des photos qui te concernent sans ton accord.
- **Droit à l'oubli :** Ce droit te permet de demander la suppression d'informations ou de publications à ton sujet qui ne te représentent plus.
- **Droit de retrait :** Ce droit te permet de retirer un contenu que tu as publié toi-même, par exemple s'il te porte préjudice.
- **Liberté d'expression :** Ce droit te permet de donner ton avis et d'exprimer tes opinions, à condition de rester respectueux ou respectueuse envers les autres.
- **Censure et modération :** La modération consiste à faire respecter les règles d'une plateforme en supprimant les contenus qui les enfreignent ; la censure limite ce que l'on a le droit de dire ou de publier.
- **Licence open source :** Une licence qui autorise à utiliser, modifier et partager librement un logiciel ou un contenu.

Séance 2 — Habitudes numériques et droit à la déconnexion

TEMPS 2.1 — Repérer et analyser ses habitudes numériques

Réponds anonymement au sondage Wooclap lancé par le professeur sur ce que tu as fait hier sur écran.

Lis la mise en situation et remplis le tableau de la page suivante.

Mise en situation

Tu analyses tes habitudes numériques. Pour chaque activité ci-dessous, décide si elle est plutôt active ou passive.

ACTIF	PASSIF
Tu **crées**, tu **produis**, tu **apprends** ou tu **participes** activement.	Tu **consommes** du contenu sans vraiment interagir ni créer.

Situations à classer

1. Coder un jeu
2. Écrire un blog ou un post
3. Faire des recherches sur le web
4. Scroller sur TikTok
5. Regarder des vidéos recommandées par YouTube
6. Créer une vidéo ou une musique
7. Regarder des Reels ou Stories
8. Utiliser une app d'apprentissage (Duolingo, Khan Academy…)
9. Lire un article ou un livre numérique
10. Regarder un live sans interagir
11. Participer à un forum
12. Organiser un événement en ligne
13. Scroller Instagram
14. Écouter de la musique en arrière-plan sans vraiment écouter

ACTIF	PASSIF

Écris le numéro de chaque situation dans la bonne colonne.

TEMPS 2.2 — Comprendre la cyberdépendance

Écoute la lecture faite par un ou une camarade volontaire. Pendant sa lecture, d'autres élèves vont l'interrompre avec de fausses notifications : observe à quel point ces interruptions perturbent la concentration.

Et à la maison ?

Il existe sur ton téléphone un mode *concentration* ou *ne pas déranger* que tu peux activer pendant que tu travailles.
Pour l'activer sur iPhone, suis ce petit guide : https://support.apple.com/fr-be/guide/iphone/iphd6288a67f/ios.
Sur Android, deux fonctionnalités sont particulièrement utiles :

- **Mode Ne pas déranger :** coupe les sons, arrête les vibrations et bloque les notifications visuelles.
- **Mode Coucher :** permet de couper les notifications (Ne pas déranger) et de passer l'écran en nuances de gris pour favoriser un meilleur sommeil.

Plus d'informations sur leur activation : https://support.google.com/android/answer/9069335?hl=fr.

TEMPS 2.3 — Cyberdépendance et droit à la déconnexion

En groupe, invente une scénette d'une à deux minutes qui illustre une situation de mauvais usage des écrans, puis joue-la devant la classe.

i Besoin d'idées ?

Voici des exemples de scénettes que tu peux reprendre ou adapter :

- Un touriste perdu en ville, anxieux car il n'a pas de connexion.
- Un repas de famille où tout le monde est sur son téléphone.
- Un groupe d'amis en récréation : chacun est sur son écran au lieu de discuter.
- Un élève qui regarde son téléphone en cours et rate une partie du cours.
- Un parent qui travaille sur son ordinateur pendant les devoirs de son enfant, sans lui accorder d'attention.
- Un ado qui scrolle sur son lit avant de dormir et a du mal à s'endormir.
- Un ado qui demande à une IA de faire ses devoirs.

Crée de l'interaction entre les personnages (fais réagir les autres) et n'hésite pas à aller dans l'excès : ta scénette doit provoquer une réaction du public (rires, réflexions…).

★ À RETENIR — HABITUDES NUMÉRIQUES

Tu peux faire deux usages d'un écran :

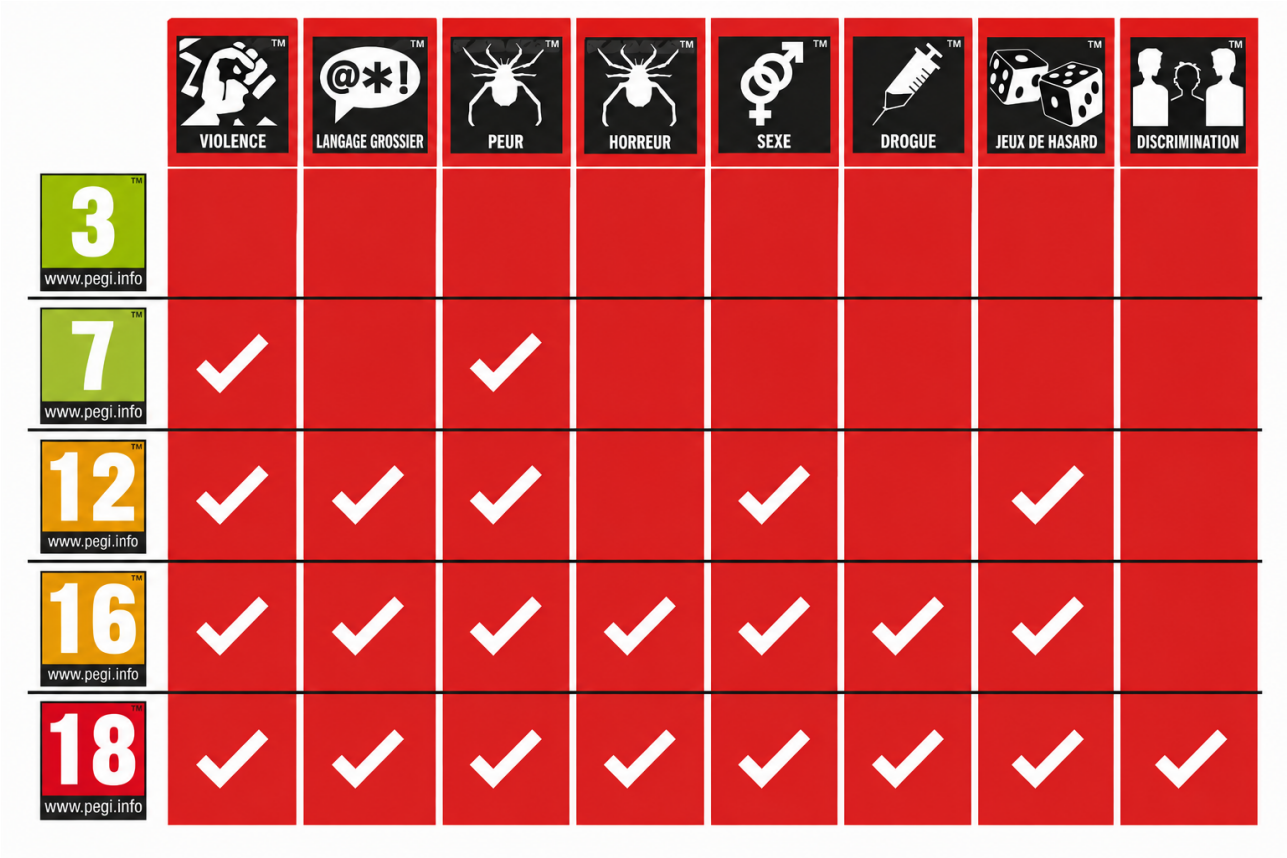
- **ACTIF :** tu crées, tu produis, tu apprends ou tu participes activement.
- **PASSIF :** tu consommes du contenu sans vraiment interagir ni créer.

La cyberdépendance, c'est une addiction aux écrans et à Internet, qui peut nuire à la santé, au sommeil ou aux relations sociales.
Le droit à la déconnexion te permet de te déconnecter des écrans pour ton bien-être. Il apporte une meilleure concentration, moins de stress, un meilleur sommeil et plus de temps pour tes relations sociales.

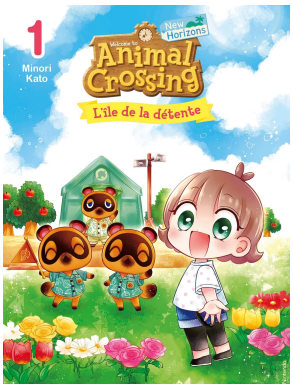
Séance 3 — Signalétique, sites sûrs et confidentialité

TEMPS 3.1 — Décoder une signalétique PEGI

Observe attentivement les symboles ci-dessous et repère ceux que tu connais déjà.



Pour chaque pochette de jeu ci-dessous, retrouve l'âge minimum recommandé et une justification basée sur les pictogrammes ou sur tes connaissances du jeu.



Nom du jeu	Âge minimum recommandé	Justification : pourquoi ?
Animal Crossing		
FC26		
Fortnite		
Minecraft		
Roblox		
Call of Duty		
GTA		
League of Legends		
Resident Evil 4		

TEMPS 3.2 — Jeu des cartes : dénicher les pièges en ligne

Avec ton binôme, tu vas recevoir un jeu de cartes préparé par le professeur. À tour de rôle : lis le message au recto d'une carte et demande-toi si c'est un piège, puis retourne la carte pour vérifier ta réponse et lire l'explication.

Quels messages t'ont trompé ? Pourquoi ? Partage tes réactions avec la classe.

TEMPS 3.3 — Un formulaire trop curieux ?

Voici un formulaire d'inscription à un jeu-concours. Entoure en vert les informations normales, en orange les informations suspectes et en rouge celles qui sont excessives.

Ensuite, mets-toi dans la peau d'un arnaqueur ou d'une arnaqueuse : que pourrait-il ou elle faire de ces informations ? Par exemple, avec ton adresse complète, il pourrait voler ton identité ou t'envoyer des colis indésirables ; avec ta photo, il pourrait usurper ton identité sur les réseaux sociaux.

GRAND JEU-CONCOURS

Tente de gagner une console de jeu !

Participation gratuite • Tirage au sort le 30 du mois

Prénom .....

Nom complet .....

Âge .....

Classe .....

Nom de ton école .....

Ville .....

Adresse de ta maison .....

Date de naissance .....

Adresse e-mail d'un parent .....

Numéro de téléphone d'un parent .....

Pseudo utilisé pour jouer en ligne .....

Ton jeu vidéo préféré .....

Couleur préférée .....

Plat préféré .....

Nom de ton animal de compagnie .....

Nom de ton meilleur ami .....

Nom de jeune fille de ta maman .....

Mot de passe de ta tablette .....

Mot de passe de ton compte de jeu .....

Code PIN de ton téléphone .....

Réponse à ta question secrète .....

Numéro de carte bancaire de tes parents .....

Photo de ta carte d'identité ☐ Joindre une photo

Signature .....

★ À RETENIR — LA SIGNALÉTIQUE PEGI

Le système **PEGI** indique l'âge minimum recommandé pour un jeu vidéo (3, 7, 12, 16 ou 18 ans), en fonction de son contenu.

- Des pictogrammes précisent le type de contenu sensible : violence, langage grossier, peur, drogue, jeux de hasard, discrimination…
- Si un jeu contient plusieurs types de contenus sensibles, c'est **l'âge le plus élevé** qui est retenu.
- Le pictogramme « Accords parentaux recommandés » signale un contenu très varié ou créé par les utilisateurs (ex. : modes de jeu personnalisés), qui ne peut pas recevoir une classification d'âge fixe.

Vérifier l'âge PEGI avant de télécharger ou d'acheter un jeu permet de choisir un contenu adapté à ton âge.

★ À RETENIR — REPÉRER UN PIÈGE EN LIGNE

Certains indices doivent t'alerter :

- Des promesses trop belles (« Tu as gagné un cadeau ! »)
- De l'urgence (« Clique maintenant ! »)
- Une demande d'informations personnelles ou de mot de passe
- Un expéditeur inconnu ou suspect
- Des liens ou des URLs étranges

Dans le doute, vérifie toujours avant de cliquer ou de répondre.
Certaines informations ne doivent **jamais** être données dans un formulaire en ligne (mot de passe, code PIN, numéro de carte bancaire, réponse à ta question secrète…), même si le formulaire semble officiel ou que le cadeau proposé est tentant.

Séance 4 — Sécurité : signaler, bloquer et protéger ses traces numériques

TEMPS 4.1 — Signaler ou bloquer un contenu

Réponds au sondage lancé par ton enseignant.

☐ J'ai déjà reçu un commentaire méchant ou un message insultant.

☐ J'ai déjà été contacté par un inconnu sur Internet.

Quelles actions concrètes peux-tu proposer pour te protéger, ou pour protéger quelqu'un d'autre, dans ce type de situation ?

TEMPS 4.2 — Phishing et cybermanipulation

Lis l'article ci-dessous, puis réponds aux questions qui suivent.

Je me suis dit : il n'y a que ma banque qui peut savoir ça : le boom des arnaques en ligne

Cet article, légèrement modifié à des fins pédagogiques, est adapté d'un reportage de France 3 Bretagne.

Jeune, à l'aise avec internet, vigilant en apparence : Hugo pensait pouvoir éviter ce genre de piège. Louise, elle, sensibilisait déjà ses équipes aux arnaques. À Namur, leurs récits racontent la même mécanique redoutable : un SMS, un appel, la pression, puis l'argent qui s'envole.

Hugo, 26 ans, victime malgré sa vigilance

Hugo (prénom d'emprunt) a 26 ans. Il vit à Namur, travaille dans un bar, commande en ligne, navigue sur internet sans difficulté. Les sites, les applis, les livraisons, les messages automatiques : tout cela fait partie de son quotidien. Il pensait savoir repérer les pièges. Il s'est fait escroquer de 1 000 euros. Et il aurait pu perdre plus.

Et pourtant, il s'est fait avoir

Tout commence après un achat en ligne. Il doit être livré. Le colis doit arriver rapidement. Puis un SMS tombe. Le message dit que « le paquet ne rentre pas dans la boîte aux lettres ». Il faut choisir un point relais. Rien de très étonnant. Le genre de contretemps banal qui arrive tous les jours.

« Je clique sur le lien. J'arrive sur le site de DHL donc oui, je me suis dit : tout est logique. »

Le lien renvoie vers une page qui ressemble à s'y méprendre à celle du transporteur. Hugo paie 1,79 euro de frais. Une somme minime. Pas de quoi éveiller immédiatement les soupçons. C'est la première brèche.

Quelques jours plus tard, un homme l'appelle. Il se présente comme un conseiller bancaire. Sa voix est posée. Son français est parfait. À l'arrière-plan, Hugo entend d'autres voix, des bruits d'ordinateur. Comme dans un bureau. Là aussi, tout semble crédible.

Le prétexte : une activité suspecte sur votre compte

Il me dit qu'on a détecté une activité suspecte sur ma carte en Allemagne. »

Le faux conseiller connaît son nom. Il a des informations personnelles. Il sait aussi qu'un paiement a été effectué via un lien reçu par SMS. Pour Hugo, l'enchaînement fait sens. Il croit parler à quelqu'un qui maîtrise la situation.

« Je me suis dit : il n'y a que ma banque qui peut savoir ça. »

Au téléphone, la pression monte. Il faut agir vite. L'homme explique que des virements suspects seraient en cours. Il faut « mettre l'argent en sécurité », le transférer vers un autre compte, le temps que la situation soit réglée. Hugo hésite. Il demande si son interlocuteur travaille vraiment chez ING. L'autre se montre presque vexé.

L'interlocuteur semble vexé et met la pression

Quand Hugo doute, l'escroc s'énerve. « Il m'a répondu d'une manière presque offusquée. En gros : on est là pour vous aider. »

La suite va très vite. Dans la panique, Hugo exécute les consignes.

« Je devais faire un virement vers un autre compte pour "sécuriser" mon argent. Il m'a volé. »

J'ai fait un premier virement de 7 000 euros. Soi-disant sur un autre compte pour mettre à l'abri l'argent de son compte courant. Avec 2 400 euros en banque, l'escroc lui demande de faire cela en deux virements. Le deuxième, de 1 400 euros, est tenté derrière. Heureusement pour Hugo, celui-là ne passe pas.

La vraie conseillère appelle également, trop tard

Deux jours plus tard, sa vraie conseillère bancaire l'appelle. Cette fois, c'est bien la bonne. Elle a repéré une activité inhabituelle sur son compte.

À ce moment-là, Hugo comprend. « Quand ma vraie conseillère m'a appelé, j'ai compris. » Il a perdu 1 000 euros. Et il sait qu'il a frôlé pire, perdre toutes ses économies.

Le rouage de l'escroquerie

Cette mécanique, les policiers de Namur la connaissent par cœur. Un SMS d'abord à propos d'un colis, d'une amende, d'un remboursement. Peu importe le prétexte. Le message contient un lien. Là se cache le premier piège.

Ils vont aspirer les premières données. Et si on règle, même une somme modique comme pour Hugo, ils vont tout avoir : numéro de compte, de carte bancaire, tout pour se faire passer pour un vrai conseiller.

Ensuite vient alors l'appel. Le faux conseiller entre en scène avec assez d'informations pour rassurer, assez d'assurance pour impressionner, assez de pression pour empêcher de réfléchir.

Selon les enquêteurs, cette escroquerie est devenue l'un des pièges du moment. Depuis le début de l'année, près de 70 personnes ont déjà porté plainte dans le district de police de Namur, soit une plainte tous les deux jours. En 2025, 177 plaintes avaient déjà été recensées. Les victimes ont tous les profils. Tous les âges. Tous les métiers. Même des policiers se sont déjà fait piéger.

Après avoir transité de compte en compte, l'argent file souvent à l'étranger. Les têtes pensantes de ces réseaux seraient basées hors de Belgique, notamment en Israël ou en Grèce, selon les enquêteurs. Des complices peuvent aussi être recrutés en Belgique, souvent via Snapchat ou Telegram.

Louise, sensibilisée mais presque piégée

Louise (prénom d'emprunt), elle, ne correspond pas non plus à l'image facile de la victime naïve. Cette cheffe d'entreprise namuroise, aujourd'hui reconvertie dans l'accompagnement des sociétés, est déjà très sensibilisée aux arnaques en ligne. Pendant des années, elle a même mis en garde ses équipes contre les fraudes et les manipulations.

« C'est moi qui organisait les séminaires contre les arnaques en ligne. »

Un scénario très élaboré pour rassurer

Elle connaît les fausses demandes de virement, les tentatives d'« escroquerie au président », les consignes de prudence. Elle sait qu'il ne faut jamais donner d'informations sensibles à un inconnu. Mais un jour de novembre, elle reçoit un SMS à propos de sa carte bancaire professionnelle. Le message annonce un paiement à l'étranger. Encore une fois, il faut cliquer sur un lien.

Là encore, tout semble solide.

Quand elle observe le site internet sur lequel elle arrive, « c'était bien floqué ING. Ça avait l'air vraiment vrai. »

Louise appelle le numéro indiqué. Au téléphone, la qualité sonore la surprend. La voix paraît lointaine. Mais son interlocuteur parle bien, sans accent marqué, et déroule son scénario avec calme. Il la rassure.

« Le design du site internet, les textes, les infos, le logo, tout paraissait vrai. »

L'escroc connaît par cœur l'appli de la banque

Il lui demande de vérifier certains éléments sur son application. La guide vers des rubriques qu'elle consulte rarement. Pose des questions précises sur ses soldes, ses encours, ses habitudes bancaires.

« L'escroc connaît par cœur l'appli de la banque. »

Il lui fait vérifier des espaces sur son appli bancaire, qu'elle ne connaît pas. Cela lui semble professionnel. « Tout était bien organisé, ça c'est sûr. »

L'escroc s'appuie aussi sur le contexte. Quelques semaines avant, une fuite de données chez Proximus a été largement médiatisée. Louise est cliente de l'opérateur. Cela renforce encore la crédibilité du discours.

Comme pour Hugo, le faux conseiller installe une forme d'emprise. Il rassure, il guide, il occupe l'espace. Puis il demande plus.

« Quand il a commencé à me demander le numéro de carte bancaire, la date de validité et le crypto, j'ai dit stop. »

Raccrocher pour se mettre en sécurité

Cette fois, Louise se reprend à temps. Le réflexe revient. Elle annonce qu'elle va appeler son vrai conseiller bancaire pour vérifier la procédure. La ligne coupe aussitôt.

« Je lui ai dit : je vais contacter mon conseiller. Et là, ça a raccroché. »

Son banquier confirme immédiatement l'arnaque. Opposition est faite dans la foulée. L'histoire s'arrête là. Sans perte d'argent. Mais avec une secousse.

« C'est tellement bien fait qu'on peut très facilement se faire avoir. »

Préjudice moyen entre 1 000 et 4 000 euros

C'est précisément ce que décrivent les enquêteurs. Les escrocs ne misent pas sur la crédulité, mais sur la pression. Ils créent un climat d'urgence. Ils donnent l'impression que le danger est immédiat. Ils parlent vite. Ils rassurent. Ils poussent à agir avant que le doute ne s'installe. Parfois, ils voient même en direct ce que la victime fait sur son écran, ce qui leur permet de commenter ses actions comme s'ils connaissaient déjà le contenu du compte.

Le plus souvent, les préjudices tournent entre 1 000 et 4 000 euros, selon les plafonds bancaires. Et dans bien des cas, les banques refusent de rembourser, estimant que les opérations ont été validées volontairement.

Conclusion : « On est tous vulnérables »

Hugo, lui, regarde désormais chaque SMS autrement. Parce qu'au fond, dans cette arnaque, tout est fait pour ressembler à la vraie vie : un colis qu'on attend, une banque qui appelle, une urgence à régler. C'est pour cela qu'elle fonctionne. Et c'est aussi pour cela qu'elle piège autant.

Le conseil des policiers tient en quelques mots : ne jamais cliquer sur un lien reçu par SMS, raccrocher en cas d'appel suspect, puis rappeler soi-même sa banque. Car un conseiller bancaire ne demandera jamais d'effectuer un virement urgent au téléphone.

Réponds à ces questions.

1. Comment les escrocs sont-ils entrés en contact **la première fois** avec Hugo ?

2. Comment sont-ils entrés en contact **la deuxième fois** ?

3. Pourquoi Hugo a-t-il cru à ce deuxième contact ?

4. Quel mécanisme psychologique pousse Hugo à agir malgré ses doutes ?

5. Le premier contact (un SMS à propos d'un colis) est à éviter. Quelles sont les **autres techniques ou prétextes** observés par les policiers de Namur ?

TEMPS 4.3 — HTTP et HTTPS

HTTP et HTTPS sont des protocoles, c'est-à-dire des règles de communication entre ton appareil (ordinateur, smartphone) et un site web.

- **HTTP :** c'est comme une lettre postale envoyée sans enveloppe. Tout le monde peut la lire si elle tombe entre de mauvaises mains (par exemple un pirate sur le même réseau Wi-Fi).
- **HTTPS :** c'est comme une lettre dans une enveloppe verrouillée. Seul le destinataire (le site web) peut l'ouvrir et la lire. Tes informations (mots de passe, messages, données bancaires) sont protégées.

Comment les reconnaître ?

- **HTTP :** l'URL commence par `http://` (sans le « S »).
- **HTTPS :** l'URL commence par `https://` (avec le « S » pour **S**écurisé).

Astuce

Vérifie la présence du cadenas dans la barre d'URL avant de saisir des informations personnelles (le cadenas n'est pas toujours visible, cela dépend des navigateurs: microsoft edge, chrome, safari, etc.).

Réponds à ces deux questions.

Si tu devais entrer ton mot de passe sur un site, lequel choisirais-tu : HTTP ou HTTPS ? Pourquoi ?

Pourquoi certains sites utilisent-ils encore HTTP ?

? Le saviez-vous ?

Les dernières lettres d'une adresse Internet (comme `.be` ou `.com`) s'appellent une **extension de domaine**. Elles donnent souvent une indication sur le type de site ou son origine.

- `.com` : signifie *commercial*. À l'origine réservée aux entreprises, cette extension est aujourd'hui la plus utilisée au monde et peut être enregistrée par presque tout le monde.
- `.org` : signifie *organization*. Elle est souvent utilisée par des associations ou des ONG.
- `.be` : extension de la Belgique, largement utilisée par les sites belges.
- `.eu` : destinée aux organisations et entreprises de l'Union européenne.
- `.gov` : réservée aux sites officiels des gouvernements.
- `.edu` : utilisée principalement par des établissements d'enseignement.

L'extension d'un site peut donner un indice, mais elle ne garantit jamais qu'il est fiable ou sécurisé. Reste vigilant face à des extensions peu connues (`.xyz`, `.tk`, `.ml`…), surtout si le site utilise encore `http://` sans le **S**.

*Rends-toi sur **Have I Been Pwned** (haveibeenpwned.com) et vérifie si une adresse mail a déjà été retrouvée dans une fuite de données.*

Une adresse trouvée dans une fuite ne signifie pas forcément qu'un compte est piraté, mais cela veut dire qu'il faut changer les mots de passe réutilisés sur plusieurs sites.

TEMPS 4.4 — Paramétrer la confidentialité et découvrir FantomApp

Complète les trois missions ci-dessous.

Mission 1 — Adresse mail scolaire ou personnelle ?

Pour chaque situation, coche la bonne case.

Situation	Adresse scolaire	Adresse personnelle
Recevoir un travail envoyé par un professeur	☐	☐
Créer un compte Zalando	☐	☐
Créer un compte Instagram ou TikTok	☐	☐
Créer un compte sur un jeu en ligne	☐	☐
S'inscrire sur Microsoft Teams ou Google Classroom	☐	☐
Créer un compte Netflix ou Spotify	☐	☐

Pourquoi ne faut-il pas utiliser son adresse mail scolaire pour tous ses comptes ?

. . . . . .

. . . . . .

. . . . . .

Mission 2 — Vérifier un de tes comptes

Choisis un compte que tu utilises régulièrement (Instagram, TikTok, Snapchat, Discord, Steam, Epic Games, Google, Microsoft…).

Nom du compte : . . . . . .

Question	Ta réponse
Mon compte est-il public ou privé ?	
Qui peut voir mes publications ?	
Qui peut m'envoyer un message ?	
Mon numéro de téléphone est-il visible ?	
Mon adresse mail est-elle visible ?	
Suis-je capable de trouver facilement les paramètres de confidentialité ?	

Mission 3 — Utiliser un ordinateur partagé

Tu utilises un ordinateur de l'école ou de la bibliothèque. Coche **uniquement** les bonnes pratiques.

- ☐ Me déconnecter de tous mes comptes
- ☐ Enregistrer mes mots de passe
- ☐ Fermer toutes les fenêtres contenant mes informations personnelles
- ☐ Laisser ma messagerie ouverte
- ☐ Fermer ma session
- ☐ Vérifier qu'aucun fichier personnel n'est resté ouvert

Explique pourquoi il est important de se déconnecter :

. . . . . .

. . . . . .

. . . . . .

*Va sur **fantomapp.fr**. Trouve « Je sécurise mes réseaux », clique sur « tout voir » et sélectionne 2 de tes réseaux sociaux favoris. Lis les astuces et choisis-en 2 que tu aimerais mettre en place pour sécuriser ton compte.*

Réseau 1 choisi : . . . . . .
Astuce 1 choisie : . . . . . .
Astuce 2 choisie : . . . . . .

Réseau 2 choisi : . . . . . .
Astuce 1 choisie : . . . . . .
Astuce 2 choisie : . . . . . .

Devoir — Le traceur numérique

Pour le prochain cours, mène l'enquête sur toi-même, un membre de ta famille (avec son accord) ou une personnalité publique, à l'aide des outils de recherche Google et des réseaux sociaux. Complète la fiche ci-dessous.
L'objectif est double : apprendre à formuler des recherches efficaces, et prendre conscience de ton empreinte numérique pour mieux protéger ta vie privée.

Nom : ..... **Prénom :** ..... **Date :** .....

1. Qui vais-je investiguer ?

Je choisis de rechercher des informations sur :

- **Moi-même**
- Un membre de ma famille (qui m'a donné son accord) : .....
- Une personnalité publique : .....

2. Les astuces de recherche Google

Exemple concret : voici à quoi ressemble une recherche Google bien formulée.

Voici les outils les plus utiles pour chercher efficacement :

- **"guillemets"** → cherche la phrase **exacte**
  Exemple : `"Marie Dupont"` trouve uniquement les pages qui contiennent exactement ces mots collés.
- **- (moins)** → exclut un mot
  Exemple : `"Marie Dupont" -Facebook` enlève les résultats qui contiennent le mot Facebook.
- **site:** → cherche uniquement sur un site
  Exemple : `site:linkedin.com "Marie Dupont"`
- **filetype:** → cherche un type de fichier
  Exemple : `"Marie Dupont" filetype:pdf`
- **OR** (en majuscules) → cherche l'un **ou** l'autre
  Exemple : `"Marie Dupont" OR "Marie D."`
- **intitle:** → le mot doit apparaître dans le titre de la page
  Exemple : `intitle:"Marie Dupont"`

3. Ma recherche sur Google

Requêtes que j'ai testées (note-en au moins 4) :

1. .....
2. .....
3. .....
4. .....
5. .....

Ce que j'ai trouvé d'intéressant (note les informations et leurs sources) :

Information trouvée	**Source (lien ou nom du site)**

Y a-t-il des informations que je n'aurais pas voulu voir apparaître ? Oui / Non – Pourquoi ? .....

.....

.....

4. Recherche sur les réseaux sociaux

J'ai regardé sur (entoure) :

Instagram TikTok Facebook LinkedIn X (Twitter) Autre : .....

Le compte est-il **public** ou **privé** ? .....

Informations visibles sans être « ami » : .....

.....

.....

.....

5. Réflexion — Vie privée et empreinte numérique

1. Parmi les informations que tu as trouvées, lesquelles te semblent **acceptables** d'être publiques ? Lesquelles devraient rester **privées** ? .....

.....

.....

2. Cinq conseils que tu donnerais à quelqu'un pour mieux protéger sa vie privée en ligne (repense à ce que tu as vu en cours et à FantomApp) :

1. .....
2. .....
3. .....
4. .....
5. .....

★ À RETENIR — SIGNALER, BLOQUER ET REPÉRER LE PHISHING

Si tu reçois un commentaire méchant, un message insultant, ou si un inconnu te contacte de façon gênante :

- **Signaler** un contenu permet d'alerter la plateforme.
- **Bloquer** une personne permet de te protéger de nouveaux contacts.
- En parler à un adulte de confiance reste une solution essentielle.

Les arnaqueurs utilisent toujours les mêmes mécanismes (**phishing**) :

- inventer un scénario de crise ou d'urgence (compte bloqué, colis en attente…) ;
- se faire passer pour quelqu'un de confiance (banque, entreprise…) ;
- utiliser des informations personnelles récupérées au préalable ;
- pousser à agir vite, sans laisser le temps de réfléchir.

Une cyberattaque ne repose pas seulement sur la technique : elle joue surtout sur tes émotions (peur, urgence, curiosité, envie de gagner quelque chose).
La règle : je reçois un message inattendu → je vérifie avant de cliquer.

★ À RETENIR — HTTP, HTTPS ET EXTENSIONS DE DOMAINE

HTTPS (avec le « S » de Sécurisé) protège les informations échangées avec un site : mots de passe, messages et données bancaires sont chiffrés. **HTTP**, sans « S », ne protège pas ces informations. Vérifie toujours la présence du cadenas avant de saisir des données personnelles.
La fin d'une adresse Internet (`.com`, `.be`, `.org`, `.eu`, `.gov`, `.edu`…) s'appelle une **extension de domaine** et peut donner un indice sur l'origine d'un site (entreprise, association, gouvernement, école…).
Attention : même une extension officielle comme `.gov` ou `.edu` ne garantit pas à elle seule qu'un site est fiable. Il faut aussi vérifier que l'adresse commence bien par `https://` et que le nom du site est correctement orthographié. Reste particulièrement vigilant face à des extensions peu connues (`.xyz`, `.tk`, `.ml`…), surtout combinées à du `http://` sans le **S**.

★ À RETENIR — PROTÉGER SES COMPTES

- Une adresse mail scolaire est destinée uniquement aux activités liées à l'école.
- Utilise plutôt une adresse personnelle pour tes comptes de jeux, de shopping ou de réseaux sociaux.
- Sur un ordinateur partagé, déconnecte-toi toujours de tes comptes et n'enregistre jamais tes mots de passe.
- Les paramètres de confidentialité te permettent de choisir qui peut accéder à tes informations.

Séance 5 — Intelligence artificielle : deepfakes, création et repères éthiques

TEMPS 5.1 — Un acteur disparu qui rejoue à l'écran ?

Regarde attentivement les trois extraits suivants. Note ce qui te semble particulier, inhabituel ou étrange.

1. Bande-annonce du film *As Deep as the Grave*
2. Extrait de *Star Wars : Rogue One* (apparition de la Princesse Leia)
3. Reconstitution par la RTBF des premières heures de la catastrophe du Bois du Cazier (8 août 1956)

Participe au débat lancé en classe à partir de ces trois extraits.

★ IMPORTANT — L'AI ACT ET LES DEEPFAKES

Depuis le 2 août 2026, l'Europe a une nouvelle règle appelée **AI Act**. Elle impose d'indiquer clairement quand une vidéo ou une image est un **deepfake** (générée ou modifiée par IA) :

- si c'est une œuvre artistique ou fictive (comme un film ou une série), il faut le mentionner, mais d'une façon qui ne gâche pas le visionnage (par exemple dans le générique) ;
- si la vidéo est présentée comme un document authentique (par exemple une fausse vidéo d'un homme ou d'une femme politique qui semble réelle), la mention doit être beaucoup plus visible et immédiate, pour ne pas tromper les gens.

Pour la reconstitution du Bois du Cazier, la RTBF a clairement indiqué qu'il s'agissait d'images générées par IA à partir de sources historiques.

TEMPS 5.2 — Une chanson réinventée par l'IA

Écoute ce morceau : une reprise de « Papaoutai » (Stromae), version Afrobeat générée par IA. Reconnais-tu la chanson ? Que penses-tu du résultat ?

Participe au débat en classe à partir de ces questions : qui a le plus contribué à cette chanson (Stromae, les développeurs de l'IA, ou la personne qui a écrit le prompt) ? Qui devrait toucher l'argent si cette musique est vendue ou diffusée ? Faut-il obligatoirement indiquer la mention « Généré par IA » ?

★ IMPORTANT — QUI DOIT SIGNALER QUOI ?

On a vu que l'Europe impose de signaler les deepfakes. Trois types d'acteurs sont concernés :

- Les **développeurs** (ceux qui créent les outils d'IA) doivent marquer techniquement les contenus, pour que les machines puissent les reconnaître.
- Les **créateurs et utilisateurs professionnels** (ceux qui publient le contenu) doivent indiquer clairement que c'est généré par IA, surtout pour les deepfakes.
- **Toi**, comme le reste du public, dois pouvoir voir facilement cette information.

TEMPS 5.3 — Comment l'IA générative apprend-elle à créer ?

Pour pouvoir générer une musique, un texte ou un visage, l'IA générative doit d'abord **s'entraîner** en analysant des millions d'exemples (chansons, styles, visages, voix…).

Le **prompt** est la consigne rédigée par l'utilisateur pour guider l'IA générative. Dans notre exemple, l'utilisateur a pu utiliser une formule comme : *« Fais une version Afrobeat de Papaoutai avec la voix de Stromae »*. L'IA générative ne « réfléchit » pas : elle associe simplement les motifs appris lors de son entraînement pour générer la réponse.

> *Réponds à cette question.*

Est-ce que l'IA générative vole la musique des artistes pour s'entraîner, ou s'en inspire-t-elle simplement, comme le ferait un être humain ?

Devoir

Pour le prochain cours, regarde la vidéo d'**OKI — RTS** consacrée au fonctionnement de l'intelligence artificielle générative, puis complète la fiche ci-dessous à l'aide des explications données dans la vidéo (et, si besoin, de recherches complémentaires). Tu peux la trouver en faisant une recherche sur internet ou en tapant ce lien dans ton navigateur: https://www.rts.ch/play/tv/oki/video/intelligence-artificielle--mais-comment-ca-fonctionne-?urn=urn:rts:video:4495dca0-47e3-3ef7-833a-ab78efbd3753.

Nom : ..... **Prénom :** ..... **Date :** .....

1. Une vidéo pour découvrir l'IA générative

Regarde la vidéo de l'émission **OKI – RTS** consacrée au fonctionnement de l'intelligence artificielle générative.

De quoi parle cette émission ? (résume en quelques phrases)

.....

.....

.....

.....

Quelle information t'a le plus étonné(e) ? Pourquoi ?

.....

.....

.....

2. Les avantages et les limites de l'IA générative

Deux avantages de l'intelligence artificielle générative :

1. .....

2. .....

Deux inconvénients ou risques liés à l'IA générative :

1. .....

2. .....

3. Quelques mots importants à comprendre

Explique **avec tes propres mots** (comme si tu expliquais à un ami ou une amie) :

IA générative : .....

.....

Prompt : .....

.....

Hallucination de l'IA : .....

.....

4. Vrai ou Faux ? Entoure et corrige si c'est faux

Pour chaque phrase, entoure **V** (vrai) ou **F** (faux). Si c'est faux, écris la correction juste en dessous.

1. L'IA ne se trompe jamais.	**V / F**
→ Correction si faux :	
2. L'IA peut t'aider à apprendre des choses.	**V / F**
→ Correction si faux :	
3. L'IA voit et entend comme nous.	**V / F**
→ Correction si faux :	
4. L'IA comprend toujours ce qu'elle dit.	**V / F**
→ Correction si faux :	
5. Parfois, l'IA invente des réponses.	**V / F**
→ Correction si faux :	
6. Pour avoir de meilleurs résultats, il est utile de donner un rôle à l'IA.	**V / F**
→ Correction si faux :	
7. Même avec l'IA, c'est toujours à moi de réfléchir et de décider.	**V / F**
→ Correction si faux :	
8. Une IA générative est entraînée avec des milliards de données.	**V / F**
→ Correction si faux :	

5. Une question que je me pose encore sur l'IA...

TEMPS 5.4 — Vers qui se tourner ?

Aujourd'hui, on peut parler à une IA quand on ne va pas bien. Pour chaque situation ci-dessous, discute en binôme : vaut-il mieux en parler à un humain, ou une IA peut-elle suffire ? Justifie ton choix.

Situation	IA ou Humain ?	Pourquoi ?
Léa rentre de l'école. Toute la journée, elle a eu l'impression d'être invisible. Personne ne lui a vraiment parlé à la pause et elle se sent seule. En arrivant chez elle, elle a envie de raconter ce qu'elle ressent à quelqu'un, juste pour ne plus garder ça pour elle.		
Adam s'est disputé avec son meilleur ami hier soir. Ils se sont envoyé des messages un peu durs et maintenant ils ne se parlent plus. Adam repasse la conversation en boucle dans sa tête et aimerait bien avoir un autre avis pour savoir comment réagir sans tout gâcher.		
Inès a un contrôle d'anglais lundi. Elle doit connaître une trentaine de mots de vocabulaire. Elle a déjà regardé sa liste deux fois, mais elle a l'impression que ça ne rentre pas bien. Elle cherche un moyen de les réviser de façon plus efficace d'ici le week-end.		
Noah est bloqué sur un exercice de maths depuis plus d'une demi-heure. Il a relu le cours, regardé l'exemple du manuel, mais il n'arrive toujours pas à comprendre la méthode. Il a l'impression de tourner en rond et voudrait qu'on lui explique autrement.		
Sarah est assise dans le couloir, juste avant un contrôle important. Son cœur bat très fort, ses mains sont un peu moites et elle a du mal à se concentrer. Elle aimerait trouver un moyen de se calmer rapidement pour pouvoir entrer dans la salle dans de meilleures conditions.		
Tom a vu une vidéo d'un petit jeu vidéo simple et il a vraiment envie d'en créer un lui-même. Le problème, c'est qu'il n'a jamais codé. Il ne sait pas par où commencer, ni quels outils utiliser, ni comment avancer étape par étape.		
Chloé regarde son agenda : elle a trois devoirs à rendre, un contrôle de sciences, un entraînement de sport et elle avait aussi promis d'aider sa sœur. Elle se sent déjà un peu débordée et aimerait trouver une façon d'organiser sa semaine pour tout faire sans s'épuiser.		

★ À RETENIR — L'AI ACT ET LES QUESTIONS ÉTHIQUES

Depuis le 2 août 2026, l'Europe impose, avec l'**AI Act**, d'indiquer clairement quand une vidéo ou une image est un deepfake (générée ou modifiée par IA). Trois types d'acteurs sont concernés : les **développeurs** (qui doivent marquer techniquement les contenus), les **créateurs et utilisateurs professionnels** (qui doivent l'indiquer clairement), et **toi**, comme le reste du public, qui dois pouvoir voir facilement cette information.
Ces nouvelles possibilités soulèvent aussi de vraies questions éthiques, sans réponse simple : qui a le droit de faire rejouer un acteur ou une actrice décédée ? Qui a le plus contribué à une œuvre recréée par IA – l'artiste original, les développeurs de l'IA, ou la personne qui a écrit le prompt ? Qui devrait toucher l'argent si elle est vendue ou diffusée ?

★ À RETENIR — COMMENT FONCTIONNE L'IA GÉNÉRATIVE

Pour générer une musique, un texte ou un visage, l'IA générative doit d'abord **s'entraîner** en analysant des millions d'exemples. Elle ne « réfléchit » pas : elle associe les motifs appris pendant son entraînement pour générer une réponse à partir d'un **prompt** (la consigne que tu lui donnes).

- **IA générative :** une intelligence artificielle qui peut créer des textes, des images, des musiques ou d'autres contenus en utilisant ce qu'elle a appris à partir de très grandes collections d'informations.
- **Prompt :** la question ou la consigne donnée à une IA. Plus le prompt est clair et précis, plus la réponse obtenue peut être utile.
- **Hallucination de l'IA :** lorsque l'IA invente une réponse fausse, mais qui semble correcte. Elle produit alors une information qui n'est pas fiable.

Séance 6 — Parcours Cyber

TEMPS 6.1 — Présentation des règles et préparation

*Vous allez jouer au **Parcours Cyber** pour réviser tout ce que vous avez appris depuis le début du module. Sur le plateau, chaque case numérotée est une case Question ; les cases rouges avec l'éclair sont des cases Imprévu.*

Règles du jeu :

1. Chaque joueur ou joueuse place son pion sur la case **Départ**.
2. À tour de rôle, on avance d'une case.
3. **Case Question** (numérotée) : quelqu'un d'autre tire une carte et lit la question à voix haute. Bonne réponse : tu restes sur la case. Mauvaise réponse : tu recules d'une case.
4. **Case Imprévu** (éclair) : tire une carte Imprévu, lis la situation et applique aussitôt l'effet indiqué (+1, +2, -1).
5. Le premier joueur ou la première joueuse qui atteint ou dépasse la case **Arrivée** gagne la partie.

TEMPS 6.2 — Partie de jeu

Vous pouvez commencer ! À chaque question ou imprévu, prends le temps d'en discuter un peu avec ton groupe avant de valider une réponse ou d'appliquer un effet.

Pendant la partie, mets de côté avec ton groupe les cartes Questions qui ont posé problème ou qui ont créé le plus de discussion.

TEMPS 6.3 — Débriefing

À la fin du jeu, choisissez une ou deux cartes parmi celles que vous avez mises de côté (celles qui vous ont paru les plus difficiles ou les plus intéressantes) et donnez-les au professeur.

Pour chaque carte lue par le professeur, essaie d'y répondre et de l'expliquer avec la classe.

★ CE QUE JE RETIENS DE CE MODULE

Parmi tout ce que tu as appris sur tes droits numériques, tes habitudes d'écran, la sécurité en ligne et l'intelligence artificielle, qu'est-ce qui t'a le plus marqué, ou qui te semble le plus utile pour la suite ?