MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE

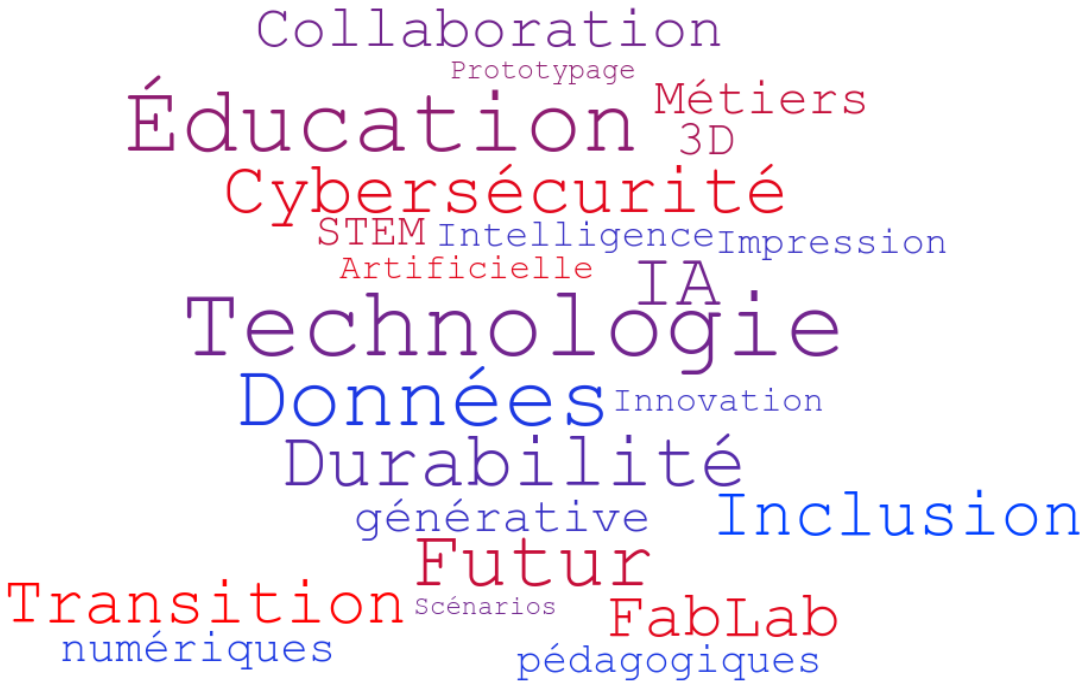
Liberté
Égalité
Fraternité

ÉduNum Technologie

N°31

Mars 2025

La **Lettre ÉduNum Technologie N°31** s'adresse aux enseignants de technologie et met en avant des thématiques comme la **cybersécurité** et l'**intelligence artificielle**. Elle propose des **séquences pédagogiques** pour sensibiliser les élèves aux risques numériques, à la protection des données et aux bonnes pratiques de cybersécurité, notamment à travers des jeux éducatifs. La lettre explore également **Vittascience**, plateforme éducative pensée pour la programmation et l'expérimentation en classe, l'accompagnement des projets innovants, comme l'utilisation de drones en agriculture. Elle présente enfin la **communauté de réflexion en éducation sur l'intelligence artificielle** (CREIA) lancée par la direction du numérique pour l'éducation (DNE).



SOMMAIRE

Des séquences pédagogiques de formation à la cybersécurité

L'enseignement de la cybersécurité dans le programme de technologie du cycle 4 contribue à préparer les élèves à relever les défis d'un monde numérique en perpétuelle évolution. Cet apprentissage s'inscrit dans une approche globale des systèmes d'information et des objets connectés, tels que décrits dans le thème « Usages et impacts sociétaux du numérique ». Les élèves découvrent les bases de la protection des données personnelles, de la gestion des identités numériques et des règles permettant un usage raisonné des environnements numériques. En cohérence avec les démarches de projet et d'investigation, ils développent des compétences pratiques en programmation et en sécurisation des objets techniques ainsi que la pensée informatique. L'objectif est de les initier à une réflexion critique sur les enjeux sociétaux du numérique, tout en renforçant leur autonomie pour interagir de manière responsable et sécurisée dans le cyberespace.

Le référentiel pour sécuriser l'environnement et les pratiques numériques élaborés dans le cadre d'un partenariat entre l'Agence nationale de sécurité des systèmes d'information (ANSSI), Cybermalveillance.gouv.fr et Pix donne une vision précise et structurée des compétences que les élèves doivent acquérir au cours de leur scolarité dans ce domaine.

Plusieurs académies ont produit des ressources, principalement des scénarios pédagogiques qui visent certaines compétences numériques en matière de sécurité informatique. Sous forme de jeu, de séances, de fiches de synthèse, ces exemples illustrent comment ce domaine peut être travaillé en classe. Ces ressources n'ont pas pour objectif de former de futurs *hackers*, mais visent à sensibiliser les élèves aux failles des systèmes à travers des activités et à les encourager à adopter de meilleures pratiques protectrices.

À travers le jeu de cartes de l'activité 5 produit par l'**académie de Grenoble** ou la séquence de l'**académie de Normandie**, les élèves sont interrogés sur l'**authentification sécurisée**. Ces ressources visent à former les élèves sur certains facteurs qui renforcent ou fragilisent un **mot de passe** comme la **longueur**, l'utilisation de **caractères spéciaux**, et le fait d'éviter d'utiliser des mots trop simples ou liés à des données personnelles. En explorant ces aspects, les élèves prennent conscience des **vulnérabilités** et des risques d'**attaques**, notamment par **force brute** ou **hameçonnage**.

En classe de 4e, l'**académie de Normandie** propose dans cette séquence aux élèves de répondre à la problématique « Comment retrouver le propriétaire d'une clé USB ? ». Elle aborde la notion de *métadonnée* en demandant aux élèves de retracer le parcours de voyage du propriétaire et de réaliser une affiche sur la machine à café pour le retrouver en utilisant les coordonnées GPS des différentes images présentes sur la clé USB. En questionnant le rôle des **antivirus**, leurs principales fonctionnalités et leur capacité à détecter, bloquer et supprimer les **logiciels malveillants**, cette ressource vise à enseigner les **bonnes pratiques** comme la mise à jour régulière des bases de données virales et l'analyse des fichiers enregistrés sur un support amovible.

Cette séquence invite les élèves à répondre à cette problématique : « Comment transférer des données personnelles du collège à la maison ou inversement en toute sécurité ? ». Elle fait s'interroger l'élève sur les façons de transférer des *données personnelles* en toute sécurité entre le collège et la maison, et prendre conscience des risques liés à l'utilisation de supports amovibles sur les réseaux. Il découvre comment utiliser son ENT pour transférer et stocker ses fichiers de manière sécurisée et explore le rôle d'une *station blanche*. Elle permet également aux élèves de se familiariser avec les notions de **connexion sécurisée** en comprenant l'importance du **protocole HTTPS** et en apprenant à **vérifier l'identité certifiée d'un site web**. Ils sont aussi amenés à **évaluer les risques liés à l'utilisation d'une connexion Internet non sécurisée**, afin d'adopter des comportements responsables en ligne.

Au cours de cette séquence pédagogique, les élèves doivent **accéder à la caméra de surveillance de l'imprimante 3D** et récupérer un fichier sur le serveur **Nextcloud** du professeur. À travers ce défi, les élèves apprennent à **reconnaître et se connecter à un réseau Wi-Fi sécurisé**, en comprenant les modalités de protection comme le chiffrement et l'authentification. Ils prennent aussi conscience des **risques liés aux réseaux Wi-Fi ouverts**, souvent utilisés dans les lieux publics, et des menaces qu'ils représentent pour les **données personnelles**.

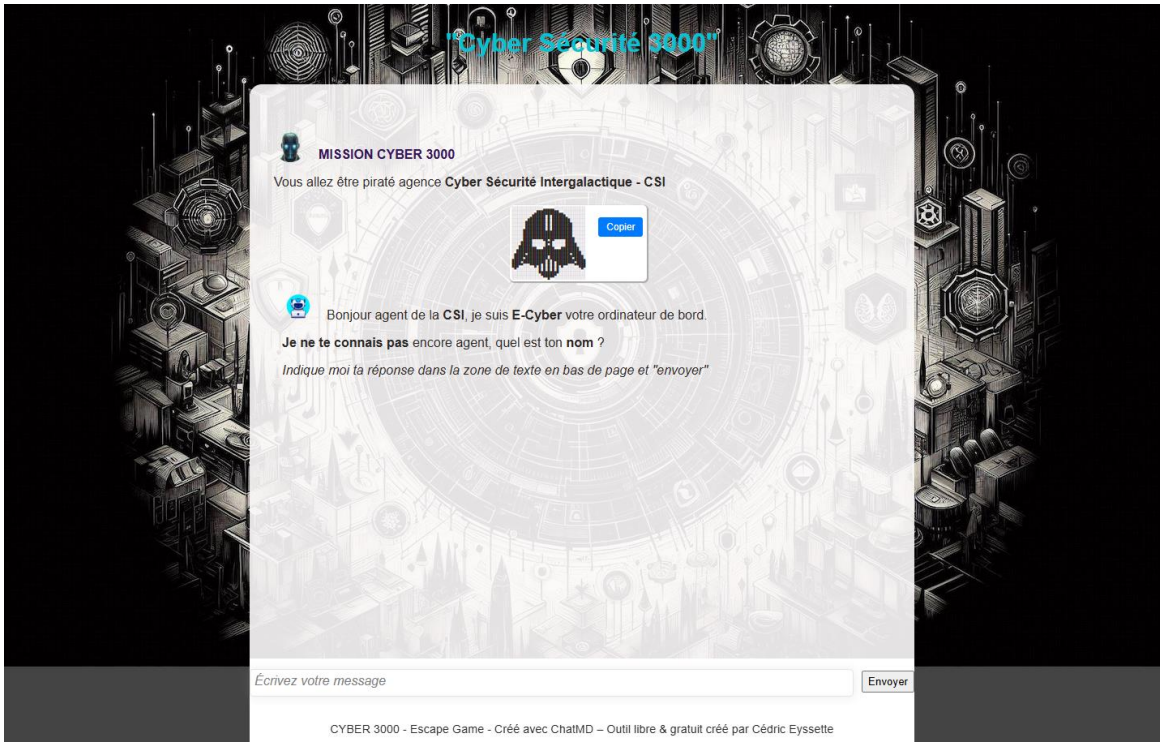
Sensibiliser aux risques de l'utilisation malveillante des traces

Chacune de nos actions sur Internet, qu'il s'agisse de publications sur les réseaux sociaux, de commentaires sur des forums, de photos ou de vidéos partagées, laisse une empreinte numérique. Ces *traces*, fréquemment considérées comme anodines, s'accumulent pour former un véritable « inventaire » en ligne. Le renseignement d'origine sources ouvertes (ROSO ou OSINT en anglais), est une technique de collecte et d'analyse d'informations publiques disponibles en ligne. Comme le montre la vidéo pédagogique de la CNIL, un individu mal intentionné peut utiliser

ces outils pour reconstituer un profil détaillé à partir de fragments d'informations volontairement ou involontairement communiqués. La facilité avec laquelle des informations personnelles peuvent être collectées et recoupées soulève de sérieux problèmes de cybersécurité. Les données, même celles supposées anodines, peuvent être utilisées pour reconstituer un profil individuel détaillé et porter atteinte à la vie privée. Il est donc crucial d'être conscient des risques et de prendre les mesures nécessaires de protection.

Découvrir des notions de la cybersécurité avec un jeu d'évasion

L'**académie de Poitiers** propose une ressource innovante pour aborder la cybersécurité avec ses élèves : le jeu CYBER 3000. Conçu sous la forme d'un dialogueur interactif, ce jeu, adapté pour les élèves de 3e, permet aux élèves de découvrir des notions essentielles.



Académie de Poitiers - Un chatbot personnalisé avec ChatMD

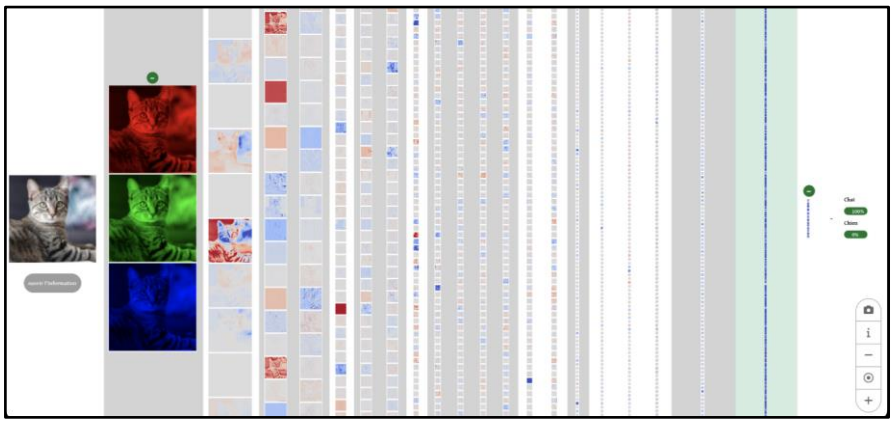
Il permet d'aborder la *citoyenneté numérique* en sensibilisant les élèves aux comportements responsables en ligne et la sécurité informatique, par exemple l'*hameçonnage* (*phishing*), la *stéganographie* ou la *protection des données* avec l'appui des compétences du CRCN en *information et données*, *communication et collaboration* ou *protection et sécurité*. Ce jeu a été développé à l'aide de deux outils *open source* : *CodiMD* (apps.education.fr) pour l'édition collaborative en temps réel de texte au format *Markdown* et *ChatMD* (Forge des communs numériques éducatifs) pour la création d'agents conversationnels personnalisé à partir d'un fichier en *Markdown*. Les auteurs ont également mis à la disposition des enseignants un document d'accompagnement qui explique en détail comment les énigmes ont été conçues, et comment les

différents mécanismes de jeu ont été mis en place. Il facilite la prise en main et donne des conseils sur la façon de l'adapter pour créer son propre jeu d'évasion.

USAGES ET EXPÉRIMENTATIONS

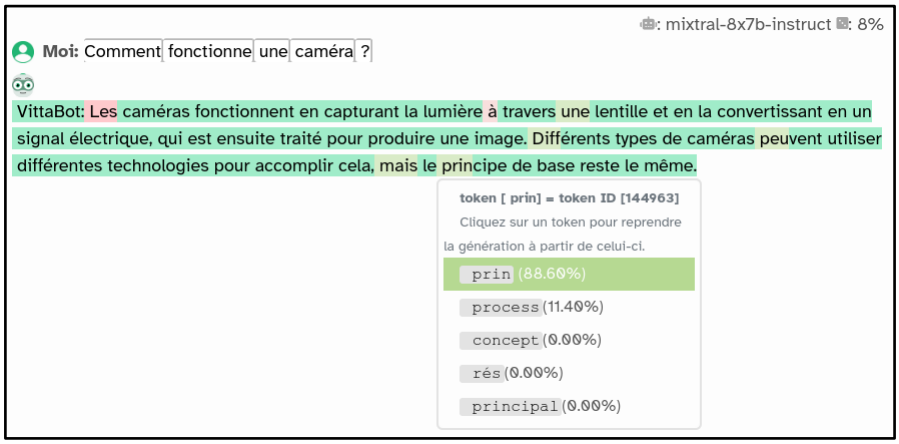
La plateforme Vittascience

Vittascience est une plateforme très utilisée par les enseignants de technologie pour sa capacité à programmer divers types de cartes, soit en **blocs visuels**, soit en **langage textuel**. Elle offre également une fonctionnalité de simulation, permettant aux élèves de tester et valider leurs solutions même sans disposer du matériel physique. En 2023, *Vittascience* introduit un module d'IA intégrant la reconnaissance d'images, de sons et de postures. Ces outils permettent d'entraîner des modèles avec des jeux de données, de les tester et de les utiliser dans le module *Adacraft*, par exemple. Ils offrent aux élèves une exploration interactive, en montrant les zones d'interaction influençant les décisions du système et en visualisant la **structure du réseau de neurones** du modèle entraîné.

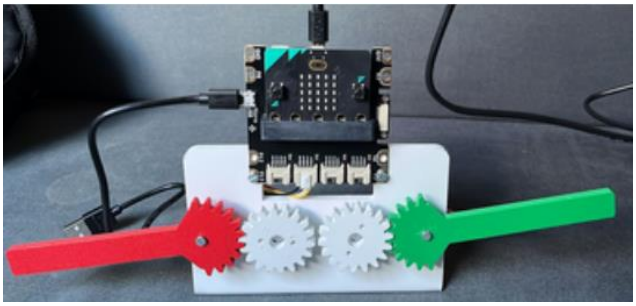


Vittascience a récemment introduit des modules d'IA dite générative pour le texte et l'image. Ces outils permettent de créer du contenu à partir de prompts en utilisant différents modèles comme *GPT, Llama, DeepSeek* ou *Stable Diffusion*. Les utilisateurs peuvent donc tester différents modèles, mais aussi ajuster le niveau de réponse aléatoire pour la génération de texte et le niveau de « guidance » pour la génération d'image afin d'affiner les résultats.

Avec des exemples simples, les élèves découvrent comment fonctionne un système génératif textuel et analysent précisément le processus de création, tout en observant l'impact des différents paramètres initiaux sur les résultats produits.



Nouvelles ressources

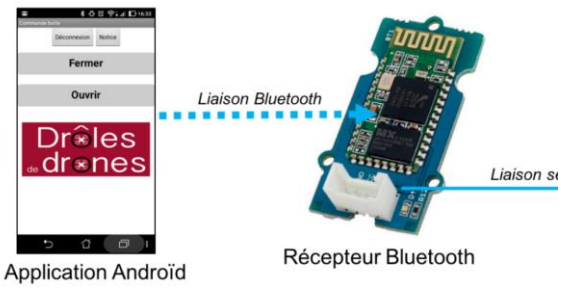


Académie de Rennes – La barrière intelligente

Cette nouvelle ressource référencée dans Édubase proposée par l'**académie de Rennes** demande aux élèves d'identifier et de corriger les dysfonctionnements d'une barrière de parking. Composée de six séances progressives d'une heure, cette séquence permet de découvrir l'usage de l'IA à travers l'interface de *Vittascience* mais aussi d'initier les élèves à l'utilisation du matériel de fabrication disponible dans le laboratoire de technologie (imprimante 3D, découpeuse laser, fraiseuse à commande numérique).

Ce projet, né d'un partenariat entre un collège et les élèves de terminale STI2D d'un lycée de l'**académie de Versailles**, montre un exemple de liaison collège/lycée. Face aux défis environnementaux et sanitaires posés par l'agriculture conventionnelle, les élèves ont conçu un système ingénieux, à savoir un drone capable de transporter des insectes auxiliaires et de les lâcher avec précision dans des zones ciblées, parfois difficiles d'accès. Cette solution de lutte biologique, respectueuse de l'environnement, consiste à utiliser des insectes bénéfiques pour contrôler les populations d'insectes nuisibles.

Le projet développe chez les élèves des compétences variées, allant de la modélisation 3D à la programmation (programme *AppInventor* pour le pilotage du drone), en passant par l'électronique et la biologie. Il s'inscrit dans une démarche de **développement durable** et de sensibilisation aux enjeux de l'agriculture biologique.



Académie de Versailles – Drôle de drone

La communauté de réflexion en éducation sur l'IA

La CREIA, ou communauté de réflexion en éducation sur l'intelligence artificielle, est une initiative lancée par la direction du numérique pour l'éducation (DNE) en novembre 2023. Elle a pour objectif principal de placer l'intelligence artificielle au centre des réflexions et des pratiques éducatives.

La CREIA se définit comme une communauté d'apprentissage entre pairs, ouverte à tous les membres de la communauté éducative. Elle vise à accompagner les changements induits par l'IA dite générative dans le système éducatif et considère l'IA comme un outil favorisant l'inclusion, l'innovation et l'amélioration continue des pratiques pédagogiques.

La CREIA met à disposition des ressources et propose des actions variées : veille informationnelle, mise à disposition de documents de référence, forums de discussion pour les échanges, micromodules de formation, conférences, animation d'un réseau de plus de cent formateurs issus des DRANE et des opérateurs de l'éducation nationale. En créant une émulation entre les académies, la CREIA vise à mettre en commun des compétences et la création d'actions de formation communes en collaborant avec la recherche (GTnum).

Les métiers du numérique et de la technologie

Les cours de technologie sont aussi une porte d'entrée vers le monde professionnel, un espace où les élèves peuvent commencer à construire leur **parcours Avenir**. Il est essentiel que ces cours offrent aux élèves un aperçu des métiers possibles. Cela répond à plusieurs objectifs : susciter des vocations en présentant la diversité des carrières possibles, développer une culture technologique en familiarisant les élèves avec les enjeux du secteur, préparer l'orientation en aidant les jeunes à identifier leurs centres d'intérêt et en luttant contre les stéréotypes. Cet article de l'ONISEP traite des métiers permettant d'inventer les technologies du futur, gérer des systèmes d'informations ou agir contre l'illectronisme.

POUR ALLER PLUS LOIN

Les femmes en technologie

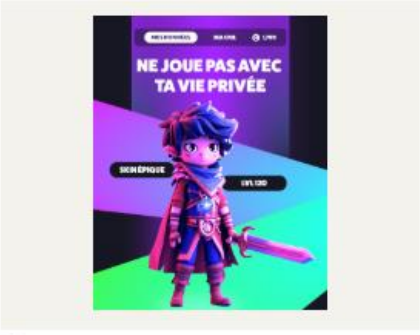
Le réseau « Femmes de Tech » de l'Académie des Technologies met en lumière des femmes inspirantes dans le domaine technologique, parrainées par des académiciens et académiciennes. Il promeut les carrières scientifiques et techniques auprès des jeunes tout en valorisant la diversité et l'échange d'expériences. Ce projet met également en avant des figures historiques comme **Émilie du Châtelet**, pour illustrer l'impact des femmes dans les sciences et la technologie. L'association « Prologin » met en place les stages « Girls Can Code ! » pour encourager les jeunes filles à s'initier à la programmation.

Ces stages couvrent divers domaines de l'informatique, tels que le développement web, la robotique et les microcontrôleurs, avec pour objectif de fournir aux participantes une base solide en programmation. La démarche de « Prologin » s'inscrit dans une volonté de promouvoir la diversité dans le secteur de l'informatique, où seulement 18% des ingénieurs sont des femmes selon l'INSEE en 2019.

GIRLS CAN CODE!

Cybersécurité

La CNIL propose par ailleurs de nombreuses ressources pour aborder le thème de la cybersécurité, mais aussi le cyberharcèlement à destination des élèves et des parents.



JEUX VIDÉO - NE JOUE PAS AVEC TA VIE PRIVÉE

MANGA - TES DONNÉES, TES DROITS

[POSTER] CYBER RÉFLEXES : SE PROTÉGER SUR INTERNET

CNIL - Médiathèque

Lettre ÉduNum proposée par la direction du numérique pour l'éducation
Sous-direction de la transformation numérique (DNE – TN3)

✉ Contact courriel

Vous recevez cette lettre car vous êtes abonné à la lettre ÉduNum Technologie
Souhaitez-vous continuer à recevoir la lettre ÉduNum Technologie ?
Abonnement/Désabonnement

À tout moment, vous disposez d'un droit d'accès, de rectification et de suppression des données qui vous concernent (articles 15 et suivants du RGPD).
Pour consulter nos mentions légales, cliquez ici.

ISSN 2739-8986 (en ligne)