Rapport sur l'IA dans les écoles
Équilibrer l'adoption et le risque

Octobre 2025

Présentation

L'intelligence artificielle (IA) transforme l'éducation. Les enseignants l'utilisent pour planifier les cours, rédiger des communications et analyser les performances des élèves. Les étudiants se tournent vers l'IA pour la recherche, le brainstorming et les projets créatifs. Dans toutes les salles de classe, la technologie libère du temps et crée de nouvelles possibilités d'apprentissage.

Pourtant, l'adoption est plus rapide que la préparation. De nombreuses écoles (41 %) déclarent avoir déjà été confrontées à des cyberincidents liés à l'IA, allant de campagnes d'hameçonnage à des contenus nuisibles générés par les élèves. Si la sensibilisation aux risques est élevée, les politiques restent incohérentes et la confiance dans la reconnaissance des menaces est très variable.

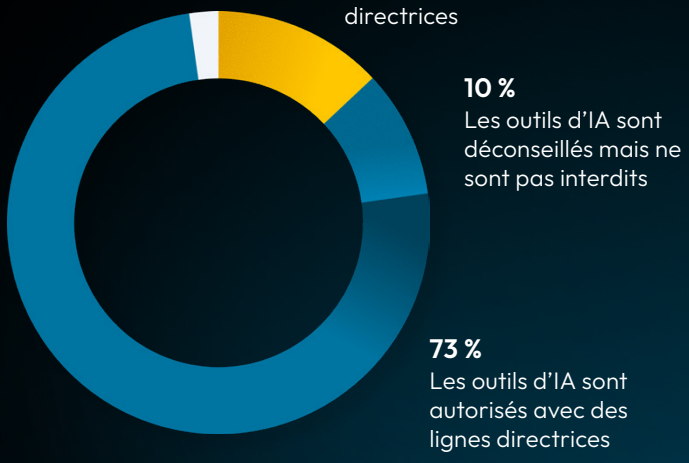
Ce rapport, qui s'appuie sur une enquête menée auprès de plus de 1 400 chefs d'établissement d'enseignement primaire, secondaire et supérieur aux États-Unis et au Royaume-Uni, examine la manière dont l'IA est actuellement utilisée dans les écoles, les mesures de protection mises en œuvre, les lacunes qui restent et les mesures que les établissements peuvent prendre pour s'assurer que l'IA renforce l'éducation au lieu de la perturber.

L'IA Est La Norme Dans Les Salles De Classe et Les Facultés

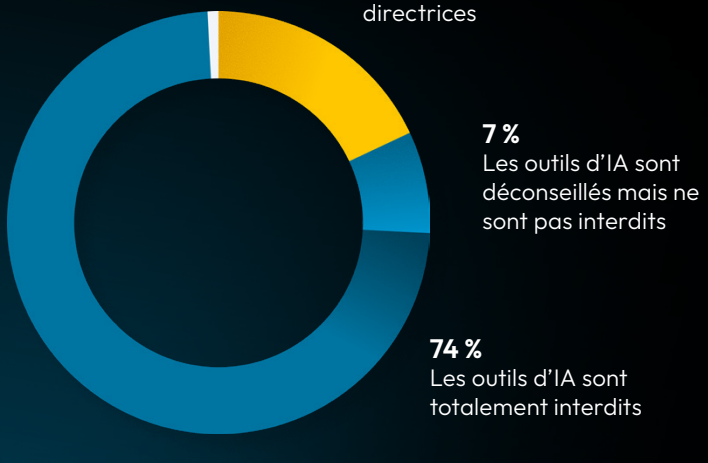
L'IA fait désormais partie intégrante des salles de classe et des bureaux des professeurs. Environ 86 % des établissements autorisent les étudiants à utiliser des outils d'IA, tandis que seuls 2 % les interdisent complètement. Chez les enseignants, le taux d'adoption est encore plus élevé (91 %), souvent avec les lignes directrices mises en place.

Les étudiants utilisent l'IA principalement pour des tâches de soutien et d'exploration. Les utilisations les plus courantes sont la recherche (62 %), le brainstorming (60 %) et l'assistance linguistique (49 %). Les projets créatifs (45 %) et l'aide à la révision (40 %) suivent, tandis que les utilisations plus sensibles comme le codage (30 %) et la réalisation de travaux (27 %) sont plus étroitement contrôlées.

Quelle est la position actuelle de votre établissement sur l'utilisation des outils d'IA par les étudiants ?



Quelle est la position actuelle de votre établissement sur l'utilisation des outils d'IA par les enseignants et le personnel ?

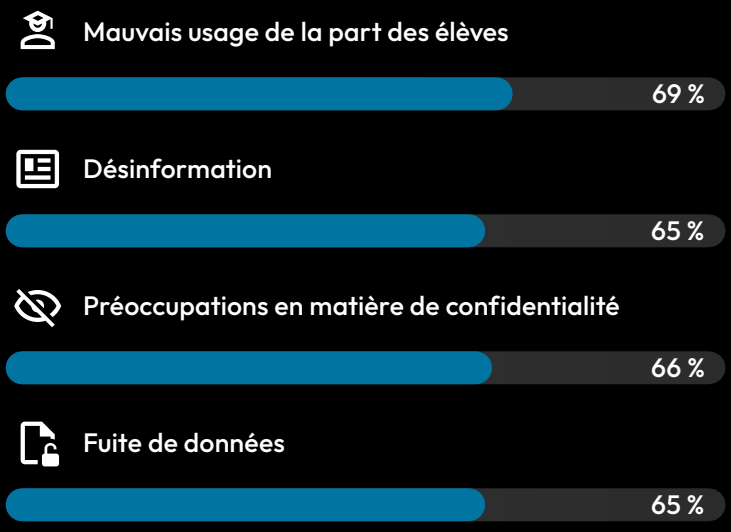


L'adoption par les enseignants est motivée par l'efficacité. Les fonctions administratives telles que la programmation (67 %) et la préparation des cours (60 %) sont les principales utilisations. Près de la moitié des établissements autorisent leur personnel à utiliser l'IA pour la notation, les stratégies d'engagement des étudiants et l'analyse des données.

Ces données montrent une division claire : les écoles soutiennent l'utilisation de l'IA pour améliorer la productivité du personnel, tout en limitant l'utilisation de l'IA par les étudiants à des activités exploratoires afin de préserver l'intégrité de l'enseignement.

Niveaux de Confiance Variés Dans La Reconnaissance des Menaces Liées à l'IA

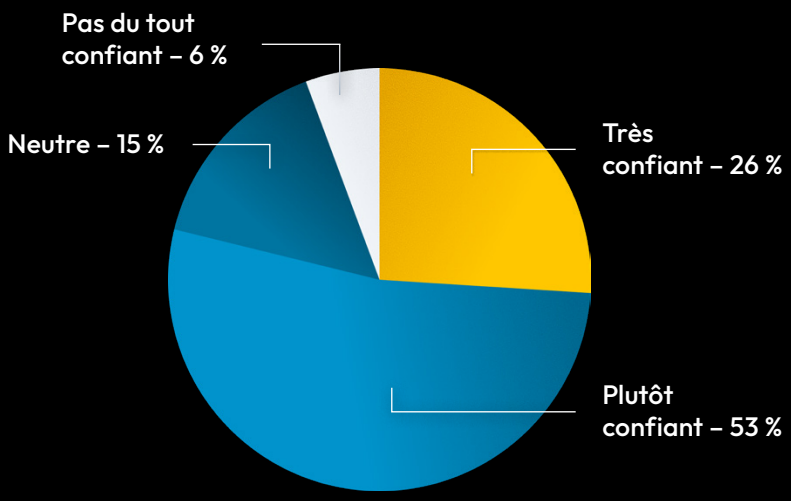
Quels sont les risques de cybersécurité liés à l'IA dont vous êtes conscient ?



La sensibilisation aux risques potentiels de cybersécurité liés à l'IA est rassurante (83 %), mais la compréhension est déséquilibrée.

Si beaucoup disent qu'ils reconnaissent les risques courants liés à l'utilisation de l'IA, tels que la fuite de données, les problèmes de confidentialité et la diffusion potentielle de fausses informations, ils sont moins nombreux à être conscients des menaces plus techniques ou émergentes. Selon le rapport Future of Defense de 2025 de Keeper Security, 95 % des chefs informatiques ont déclaré que les cyberattaques sont plus sophistiquées que jamais et qu'ils ne sont pas préparés à cette nouvelle vague de vecteurs de menace.

Dans quelle mesure reconnaissez-vous les cybermenaces liées à l'IA (par exemple, deepfake, hameçonnage) ?

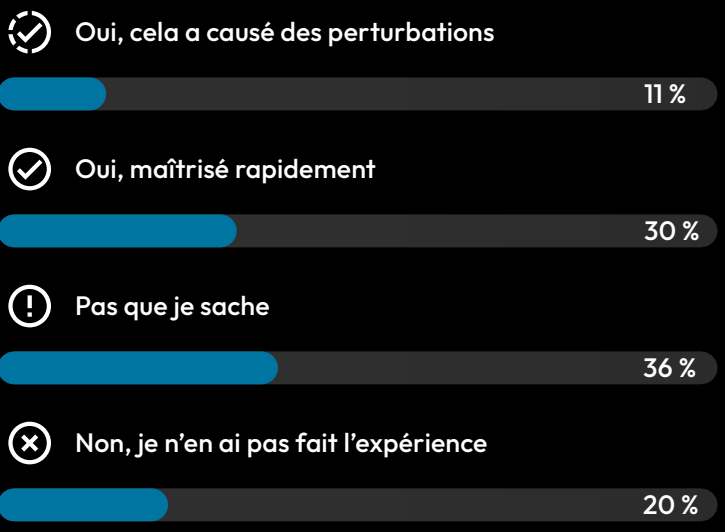


La plupart des éducateurs pensent pouvoir repérer une escroquerie à l'IA, mais seul un sur quatre se sent vraiment sûr de lui. Quand 41 % des écoles signalent déjà des cyberincidents liés à l'IA, cet écart pourrait exposer les écoles.

La combinaison d'une large sensibilisation et d'une préparation technique limitée nécessite une approche à plusieurs niveaux : combinez la formation et la sensibilisation des employés avec le chiffrement des données, la détection avancée des menaces et les contrôles d'accès (y compris les gestionnaires de mots de passe et PAM) pour prévenir les attaques basées sur l'IA et réduire l'ampleur des dégâts lorsque des incidents se produisent.

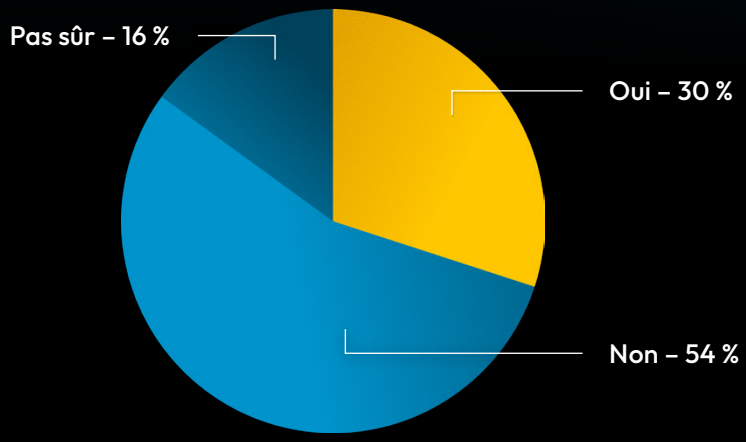
Les Incidents Liés à l'IA se Produisent Dans Les Ecoles

Votre établissement a-t-elle été la cible de tentatives d'hameçonnage ou de campagnes de désinformation générées par l'IA (par exemple, des vidéos "deepfake", des sons synthétiques) ?

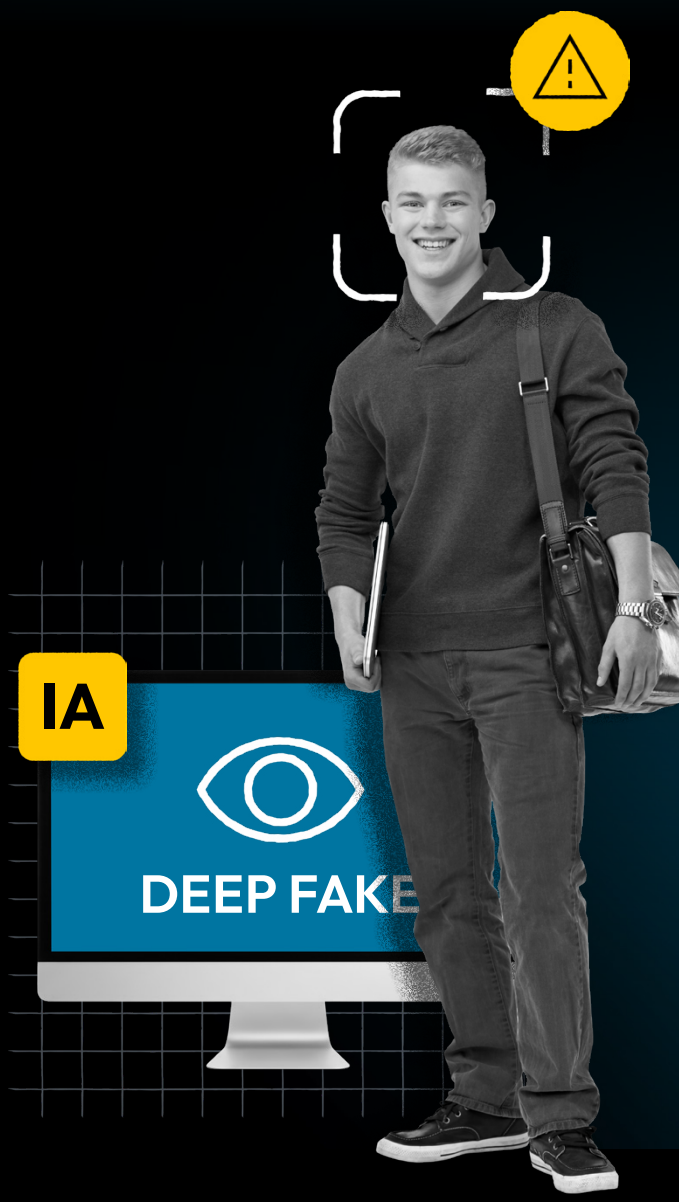


Les écoles sont déjà confrontées à des incidents liés à l'IA, tant en interne qu'en externe. Parmi les écoles, 41 % ont déclaré avoir été confrontés à des tentatives d'hameçonnage, de désinformation et d'autres actions perturbatrices, tandis que près de 30 % ont signalé des cas d'étudiants produisant des contenus IA préjudiciables. Alors que la plupart des événements confirmés ont été « maîtrisés rapidement » (30 %), la majorité des personnes interrogées (39 %) ne savaient pas si des incidents s'étaient produits, ce qui suggère des lacunes importantes en matière de suivi et de sensibilisation.

Votre école a-t-elle été confrontée à des élèves créant du contenu IA nuisible (deepfake de pairs, etc.) ?



Dans quelle mesure votre établissement est-elle prête à faire face aux menaces de cybersécurité liées à l'IA au cours des deux prochaines années ?



La plupart des établissements (82 %) ont déclaré qu'elles se sentaient au moins « plutôt préparées » pour faire face aux menaces de cybersécurité liées à l'IA, bien que ce chiffre tombe à 32 % pour celles qui se sentent « très bien préparées ». Cette confiance, tempérée par la prudence, s'aligne sur les thèmes précédents : les écoles sont conscientes des risques, mais des lacunes importantes subsistent dans la préparation générale et l'incertitude persiste quant à l'efficacité des mesures de protection existantes.

Les Problèmes de Cybersécurité

Préoccupation générale concernant les menaces de cybersécurité liées à l'IA :

37 %
Très inquiet

53 %
Plutôt inquiet

10 %
Pas inquiet

Qu'est-ce qui vous préoccupe le plus ?

65 %
Violations de la confidentialité des étudiants

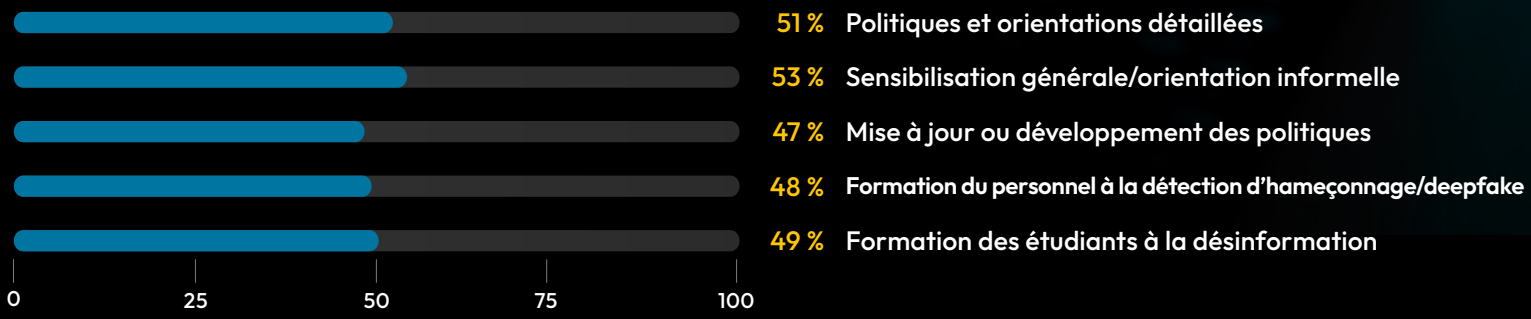
53 %
Perturbation de l'apprentissag

52 %
Usurpation d'identité de deepfake de personnel ou d'étudiants

Avec plus de 40 % déjà touchés, l'inquiétude des enseignants face aux menaces de cybersécurité liées à l'IA est, sans surprise, quasi universelle, 90 % des personnes interrogées étant au moins « plutôt préoccupées ». Plus d'un tiers (37 %) se sont déclarés « très inquiets », avec la sécurité des étudiants et les résultats de l'apprentissage - y compris les violations de la confidentialité, l'usurpation d'identité deepfake et les perturbations potentielles de l'apprentissage - figurant en tête de liste de leurs inquiétudes. Les préoccupations sont également notées concernant la partialité des résultats de l'IA (43 %), les atteintes à la réputation (37 %) et les préjudices financiers (36 %), parce qu'ils menacent la résilience des opérations et de la réputation.

Les Politiques et Les Garanties Sont Fragmentées

Comment votre école ou université aborde-t-elle la question d'hameçonnage et de la désinformation générés par l'IA ?*



Même si les écoles et les universités élaborent des cadres pour régir l'utilisation de l'IA, la mise en œuvre est inégale. L'élaboration des politiques continue de rattraper la pratique : un peu plus de la moitié ont mis en place des politiques détaillées (51 %) ou des orientations informelles (53 %), tandis que moins de 60 % déploient des outils de détection de l'IA et des programmes d'éducation des étudiants. Avec plus de 40 % déjà touchés, le fait que seul un tiers (34 %) dispose de budgets dédiés et que seuls 37 % disposent de plans de réponse aux incidents indique une lacune préoccupante en matière de préparation. Les lignes directrices relatives à la protection de la confidentialité, au consentement et à la finalité éducative sont en tête des politiques actives. La grande majorité des écoles (90 %) disposent déjà d'une politique ou prévoient d'en avoir une dans les six mois à un an, bien que ce chiffre tombe à 42 % pour celles qui ont déjà une politique en place.

La perception de la fiabilité des outils de détection de l'IA est au mieux modérée : seuls 26 % les considèrent comme « très fiables » dans leur forme actuelle, ce qui souligne les limites des seules mesures de protection techniques. La formation des enseignants est répartie entre des approches formelles (37 %), basées sur les contemporains (36 %) et informelles (19 %), ce qui suggère que les établissements sont encore en train de trouver les meilleurs moyens de développer la maîtrise de l'IA et la sensibilisation à la cybersécurité.

***Statistiques supplémentaires**

Outils techniques : 20 %
Collaboration avec des partenaires extérieurs dans le domaine de la cybersécurité : 19 %
Pas de démarches en cours : 3 %

Le Chemin à Parcourir : Combler Le Fossé Entre L'Adoption et l'État de Préparation

Aujourd'hui, la question n'est pas de savoir s'il faut adopter l'IA, mais comment gouverner, sécuriser et guider son utilisation tout en contrôlant les menaces existantes et émergentes. Ce rapport montre que les établissements ont déjà pris du retard en matière de politique, de gouvernance et de budgétisation efficaces par rapport à la vitesse d'adoption de l'IA. Ce retard en matière de gouvernance, de formation et de mise à jour des mesures de sécurité pourrait s'avérer encore plus préjudiciable dans l'avenir immédiat, car les établissements déclarent déjà être confrontés à des menaces liées à l'IA et à des utilisations abusives préjudiciables.

Les données suggèrent trois impératifs clés pour les dirigeants de l'éducation aujourd'hui :

- **Combler le fossé politique :** formalisez des politiques en matière d'IA qui concilient l'adoption et l'utilisation responsable.
- **Renforcer la résilience :** investissez dans la formation, la sensibilisation, la cybersécurité et les outils de détection afin de mieux préparer le personnel et les étudiants aux menaces liées à l'IA.
- **Préserver la confiance :** abordez directement les questions de confidentialité et d'éthique, en veillant à ce que les mesures de gestion de l'utilisation de l'IA n'érodent pas la confiance des étudiants ou de la communauté.

En pratique, cela signifie qu'il faut prendre des mesures immédiates et réalisables pour renforcer les défenses :

- Renforcez l'authentification multifactorielle (MFA) dans tous les systèmes afin de réduire le risque de compromission des comptes.
- Adoptez une solution de gestion des accès privilégiés (PAM) pour contrôler qui peut accéder aux données sensibles et aux systèmes critiques.
- Enseignez au personnel et aux élèves des pratiques strictes en matière de mot de passe afin de réduire l'un des points d'entrée les plus courants pour les attaquants.
- Déployez une détection et une surveillance en temps réel pour repérer l'hameçonnage, le deepfake et d'autres nouvelles menaces basées sur l'IA avant qu'elles ne prennent de l'ampleur.
- Examinez et mettez régulièrement à jour les politiques en matière d'intelligence artificielle pour vous assurer qu'elles sont adaptées aux nouvealles technologies, risques et cas d'utilisation dans la salle de classe.

Pour les écoles et les universités, les deux prochaines années seront cruciales pour décider si l'IA devient un partenaire de confiance dans l'éducation ou une vulnérabilité permanente. En prenant ces mesures proactives dès maintenant, les institutions peuvent suivre le rythme d'adoption tout en gardant une longueur d'avance sur l'évolution du paysage des menaces.

Méthodologie

Keeper Security est un acteur innovant en matière de cybersécurité et fournisseur de la plateforme de gestion des accès privilégiés (PAM) zero trust et zero knowledge qui a demandé à l'agence de recherche indépendante TrendCandy de mener une enquête auprès de 1 460 administrateurs d'établissements d'enseignement aux États-Unis et au Royaume-Uni sur la façon dont les écoles adoptent et utilisent l'IA et se préparent à la cybersécurité.

L'enquête en ligne, rémunérée, s'adressait aux principaux responsables des établissements d'enseignement aux États-Unis et au Royaume-Uni, conformément à des exigences strictes en matière de méthodologie d'enquête, notamment l'échantillonnage aléatoire, les pratiques en double aveugle et les contrôles de la qualité des données.

La marge d'erreur pour cette étude est de +/- 3 % au niveau de confiance de 95 %.

À propos de Keeper Security

Keeper Security transforme la cybersécurité pour des millions d'individus et des milliers d'organisations dans le monde. Construite avec un chiffrement de bout en bout, la plateforme de cybersécurité intuitive de Keeper protège chaque utilisateur, sur chaque appareil, en chaque lieu. Notre solution brevetée de gestion des accès à privilèges Zero-Trust et Zero-Knowledge unifie la gestion des mots de passe, des secrets et des connexions avec isolation du navigateur à distance. En combinant ces composants de gestion essentiels de l'identité et des accès en une seule solution cloud-based, Keeper offre une visibilité, une sécurité et un contrôle inégalés tout en veillant à ce que les exigences en matière de conformité et d'audit soient respectées. Découvrez comment Keeper peut défendre votre organisation face aux cybermenaces sur KeeperSecurity.com.