KEEPER®

KI in Schulen Report

Die Balance zwischen Einführungund Risiko

Oktober 2025

Überblick

Künstliche Intelligenz (KI) verändert die Bildung. Lehrer verwenden sie, um Unterrichtsstunden zu planen, Mitteilungen zu verfassen und die Leistung der Schüler und Studenten zu analysieren. Lernende nutzen KI für Forschung, Brainstorming und kreative Projekte. In Klassenzimmern und im Hörsaal schafft die Technologie Zeit und neue Lernmöglichkeiten.

Dennoch übertrifft die Akzeptanz die Bereitschaft. 41 Prozent der Bildungseinrichtungen berichten, dass sie bereits KI-bezogene Cybervorfälle erlebt haben, die von Phishing-Kampagnen bis hin zu schädlichen, von Lernenden erstellten Inhalten reichen. Obwohl das Risikobewusstsein hoch ist, sind die Richtlinien nach wie vor inkonsistent und das Vertrauen in die Erkennung von Bedrohungen schwankt stark.

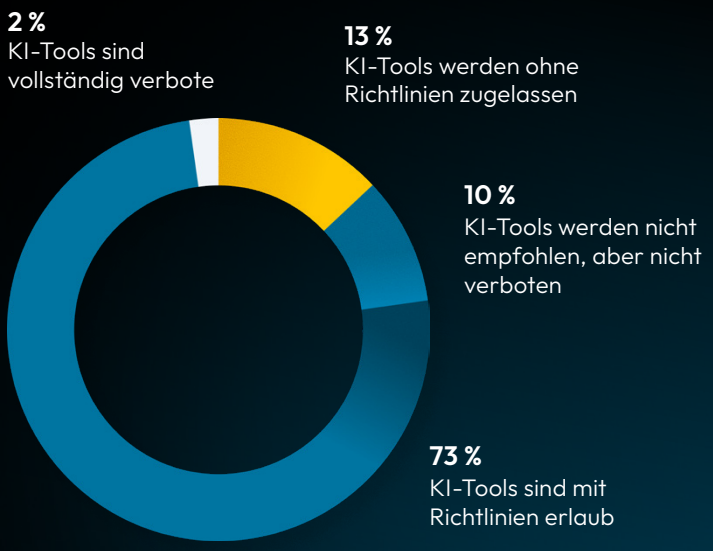
Dieser Bericht basiert auf einer Umfrage unter mehr als 1.400 Bildungsverantwortlichen aus den Bereichen Grundschule, Sekundarstufe und Hochschulbildung in den USA und Großbritannien. Er untersucht, wie KI heute in Bildungseinrichtungen eingesetzt wird, wo Sicherheitsvorkehrungen getroffen wurden, wo noch Lücken bestehen und welche Schritte Institutionen unternehmen können, um sicherzustellen, dass KI die Bildung stärkt, anstatt sie zu stören.

KI ist in Klassenzimmern und Fakultäten die Norm

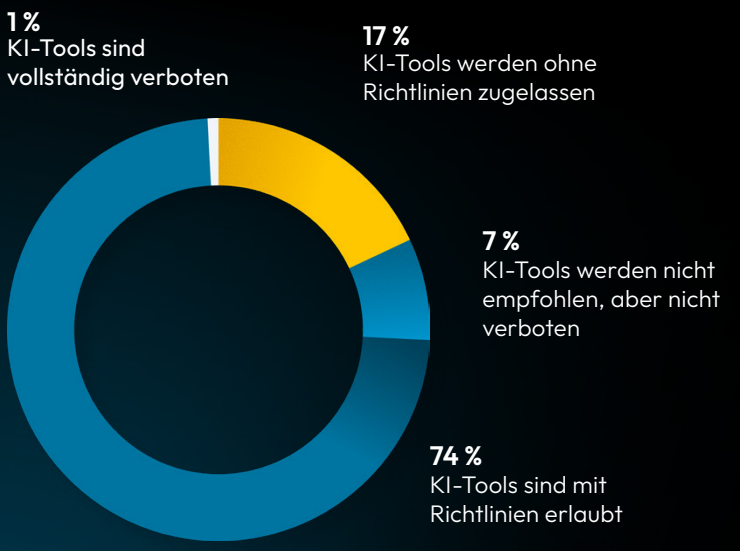
KI ist heute ein alltäglicher Bestandteil im Klassenzimmer, Hörsaal und in Fakultätsbüros. 86 Prozent der Institutionen erlauben ihren Lernenden die Nutzung von KI-Tools, während nur 2 Prozent sie gänzlich verboten haben. Unter den Fakultäten ist die Akzeptanz mit 91 % sogar noch höher, oft mit entsprechenden Richtlinien.

Lernende nutzen KI vor allem für unterstützende und explorative Aufgaben. Die häufigsten Verwendungszwecke sind Recherche (62 %), Brainstorming (60 %) und Sprachunterstützung (49 %). Es folgen kreative Projekte (45 %) und Unterstützung bei der Überarbeitung (40 %), während sensiblere Anwendungen wie das Programmieren (30 %) und das Abschließen von Aufgaben (27 %) strenger kontrolliert werden.

Wie steht Ihre Einrichtung derzeit zum Einsatz von KI-Tools durch Lernende?



Wie steht Ihre Institution derzeit zur Nutzung von KI-Tools durch Lehrkräfte und Mitarbeiter?

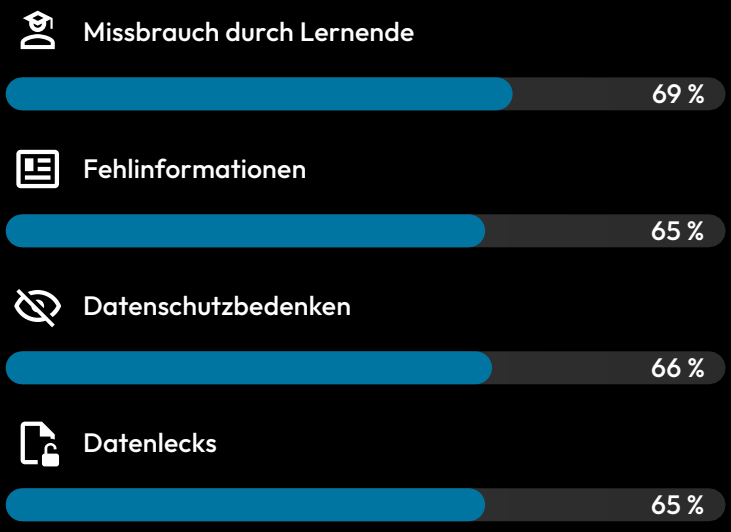


Die Akzeptanz bei Bildungseinrichtungen wird durch Effizienz bestimmt. Verwaltungsfunktionen wie Terminplanung (67 %) und Unterrichtsvorbereitung (60 %) sind die Hauptanwendungsgebiete. Etwa die Hälfte der Einrichtungen gestattet ihren Mitarbeitern den Einsatz von KI für die Benotung, Strategien zur Einbindung der Studierenden und die Datenanalyse.

Diese Daten zeigen eine klare Kluft: Die Bildungseinrichtungen ermutigen ihre Mitarbeiter, KI zur Verbesserung der Produktivität einzusetzen, während sie die Nutzung durch Lernende auf explorative Aktivitäten beschränken, um die akademische Integrität zu wahren.

Unterschiedliche Vertrauensniveaus bei der Erkennung von KI-Bedrohungen

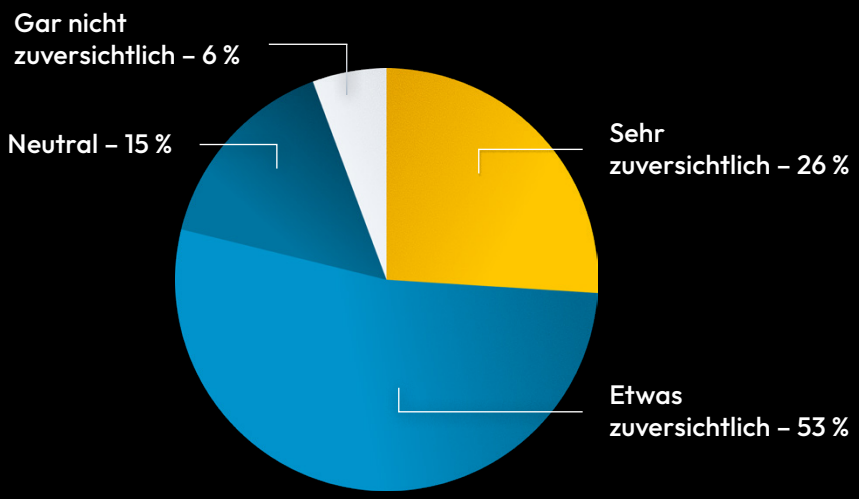
Welche KI-Cybersicherheitsrisiken sind Ihnen bekannt?



Das Bewusstsein für potenzielle KI-bezogene Cybersicherheitsrisiken ist beruhigend hoch (83 %), das Verständnis dafür ist jedoch unterschiedlich ausgeprägt.

Während viele sagen, dass sie die allgemeinen Risiken erkennen, die mit der Nutzung von KI verbunden sind, wie etwa Datenlecks, Datenschutzbedenken und die potenzielle Verbreitung von Fehlinformationen, sind sich weniger der eher technischen oder neu auftretenden Bedrohungen bewusst. Laut dem 2025 Future of Defense Report von Keeper Security gaben 95 % der IT-Leiter an, dass Cyberangriffe ausgefeilter seien als je zuvor – und dass sie auf diese neue Welle von Bedrohungsvektoren nicht vorbereitet seien.

Wie sicher sind Sie sich, KI-bezogene Cyberbedrohungen (z. B. Deepfakes, KI-gestütztes Phishing) zu erkennen?

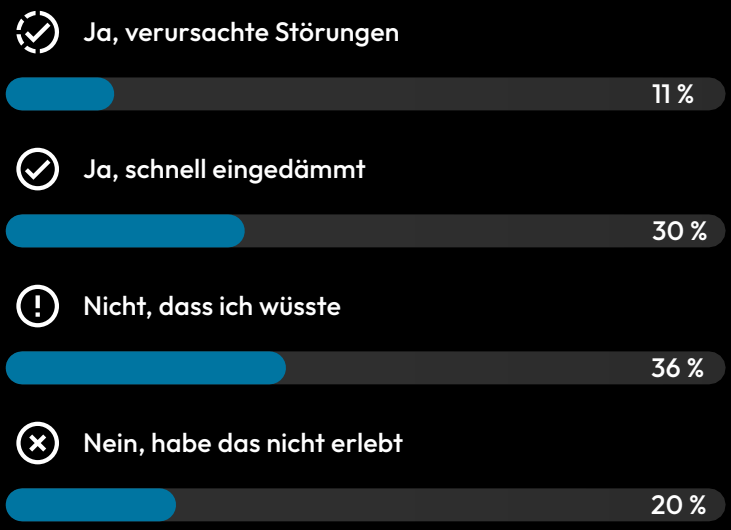


Die meisten Pädagogen glauben, dass sie einen KI-Betrug erkennen können, aber nur jeder Vierte ist sich dessen wirklich sicher. Da bereits 41 % der Bildungseinrichtungen KI-bezogene Cybervorfälle melden, könnte diese Lücke die Bildungseinrichtuingen angreifbar machen.

Die Kombination aus weit verbreitetem Bewusstsein und begrenzter technischer Bereitschaft erfordert einen mehrschichtigen Ansatz: Die Kombination aus Mitarbeiterschulung und -bewusstsein mit Datenverschlüsselung, erweiterter Bedrohungserkennung und Zugriffskontrolle (einschließlich Passwortmanagern und PAM), um KI-gestützte Angriffe zu verhindern und den Explosionsradius bei Vorfällen zu reduzieren.

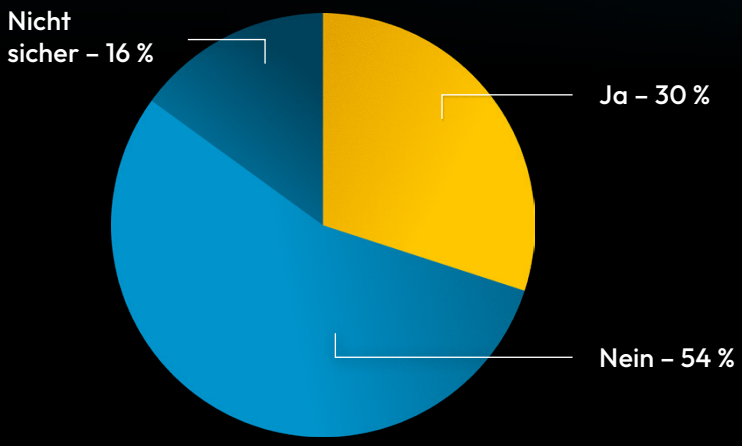
KI-bezogene Vorfälle ereignen sich in Schulen

War Ihre Institution Ziel von KI-generierten Phishing-Versuchen oder Fehlinformationskampagnen (z. B. Deepfake-Videos, synthetisches Audio)?

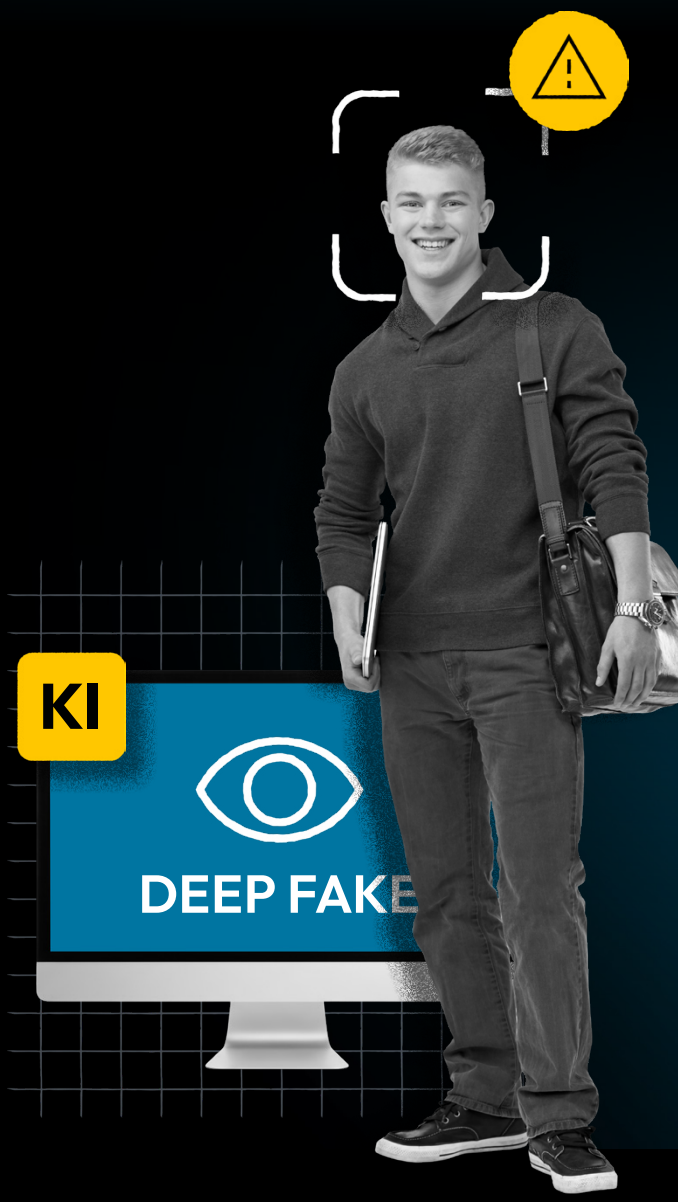


An Bildungseinrichtungen kommt es bereits zu KI-bezogenen Vorfällen, sowohl intern als auch extern. 41 Prozent gaben an, dass sie Phishing, Fehlinformationen und anderen Störversuchen ausgesetzt waren, während fast 30 Prozent von Fällen berichten, in denen Schüler schädliche KI-Inhalte erzeugt haben. Während die meisten bestätigten Vorfälle ‚schnell eingedämmt" wurden (30 %), war sich die Mehrheit der Befragten (39 %) nicht sicher, ob es zu Vorfällen gekommen war, was auf erhebliche Lücken bei der Überwachung und Sensibilisierung hindeutet.

Hat es Ihre Bildungseinrichtung erlebt, dass Lernende schädliche KI-Inhalte (Deepfakes von Mitschülern usw.) erstellen?



Wie gut ist Ihre Institution auf die Bewältigung KI-bezogener Cybersicherheitsbedrohungen in den nächsten ein bis zwei Jahren vorbereitet?



Die meisten Institutionen (82 %) gaben an, dass sie sich zumindest ‚einigermaßen vorbereitet" fühlen, um mit KI-bezogenen Cybersicherheitsbedrohungen umzugehen. Bei denjenigen, die sich ‚sehr gut vorbereitet" fühlen, sinkt dieser Wert jedoch auf 32 %. Dieses durch Vorsicht gemilderte Vertrauen steht im Einklang mit früheren Themen: Die Bildungseinrichtungen sind sich der Risiken bewusst, es bestehen jedoch weiterhin erhebliche Lücken in der allgemeinen Vorbereitung und es besteht weiterhin Unsicherheit über die Wirksamkeit der bestehenden Sicherheitsvorkehrungen.

Die Bedenken hinsichtlich der Cybersicherheit

Allgemeine Besorgnis über KI-bezogene Cybersicherheitsbedrohungen:

37 %
Sehr besorgt

53 %
Etwas besorgt

10 %
Nicht besorgt

Was bereitet Ihnen die größten Bedenken?

65 %
Verstöße gegen die Privatsphäre der Studierenden

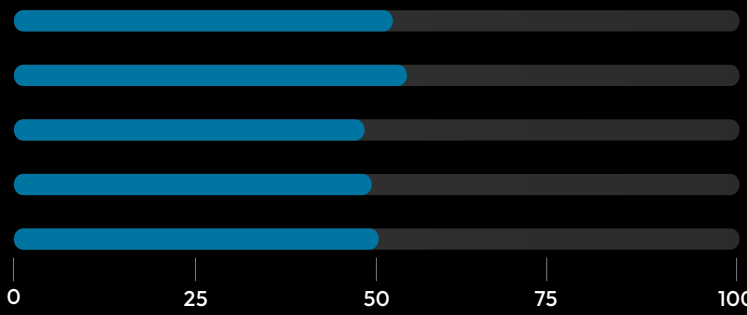
53 %
Lernunterbrechung

52 %
Deepfake-Imitation von Mitarbeitern/Studenten

Da bereits mehr als 40 % betroffen sind, ist die Besorgnis der Fakultät hinsichtlich KI-bezogener Cybersicherheitsbedrohungen - wenig überraschend - nahezu universell: 90 % der Befragten sind zumindest „etwas besorgt“. Mehr als ein Drittel (37 %) gab an, „sehr besorgt“ zu sein, wobei die Sicherheit und die Lernergebnisse der Schüler – darunter Datenschutzverletzungen, Deepfake-Identitätsdiebstahl und mögliche Lernstörungen – ganz oben auf der Liste der Ängste stehen. Darüber hinaus bestehen erhebliche Bedenken hinsichtlich der Verzerrung von KI-Ergebnissen (43 %), des Rufschadens (37 %) und des finanziellen Schadens (36 %), also Risiken, die sowohl die operative Widerstandsfähigkeit als auch die Reputation gefährden.

Richtlinien und Schutzmaßnahmen sind fragmentiert

Wie geht Ihre Schule oder Universität mit durch KI generiertem Phishing und Fehlinformationen um?*



- 51 % **Detaillierte Richtlinien/Leitfäden**
- 53 % **Allgemeines Bewusstsein/informelle Anleitung**
- 47 % **Aktualisierung oder Entwicklung von Richtlinien**
- 48 % **Schulung der Mitarbeiter zum Erkennen von Phishing/Deepfakes**
- 49 % **Aufklärung der Studierenden über Fehlinformationen/ Desinformationen**

Während Schulen und Universitäten Rahmenbedingungen für die Nutzung von KI schaffen, erfolgt die Umsetzung unterschiedlich. Die Entwicklung von Richtlinien hinkt der Praxis noch hinterher: Knapp über die Hälfte verfügt über detaillierte Richtlinien (51 %) oder informelle Anleitungen (53 %), während weniger als 60 % KI-Erkennungstools und Bildungsprogramme für Studenten einsetzen. Mehr als 40 % sind bereits betroffen, doch die Tatsache, dass nur ein Drittel (34 %) über entsprechende Budgets und lediglich 37 % über Notfallreaktionspläne verfügen, deutet auf eine besorgniserregende Lücke bei der Vorbereitung hin. Datenschutz, Einverständnis und Leitlinien für Bildungszwecke nehmen die Vorreiterrolle für aktive Richtlinien ein. Die große Mehrheit der Bildungseinrichtungen (90 %) verfügt bereits über Richtlinien oder erwartet diese innerhalb der nächsten sechs Monate bis zu einem Jahr. Bei den Bildungseinrichtungen, die bereits über eine Richtlinie verfügen, sinkt die Zahl jedoch auf 42 %.

Die Wahrnehmung der Zuverlässigkeit von KI-Erkennungstools ist bestenfalls mäßig: Nur 26 % halten sie in ihrer aktuellen Form für „sehr zuverlässig“, was die Grenzen rein technischer Schutzmaßnahmen hervorhebt. Die Ausbildung der Lehrkräfte erfolgt in formellen (37 %), peer-basierten (36 %) und informellen (19 %) Ansätzen. Dies lässt darauf schließen, dass die Institutionen noch immer mit den besten Methoden experimentieren, um KI-Kompetenzen und ein Bewusstsein für Cybersicherheit aufzubauen.

***Zusätzliche Statistiken**

Technische Werkzeuge: 20 %
Zusammenarbeit mit externen Cybersicherheitspartnern: 19 %
Ergreift derzeit keine Maßnahmen: 3 %

Der Weg in die Zukunft: Die Lücke zwischen Akzeptanz und Bereitschaft schließen

Die Frage lautet heute nicht, ob KI eingeführt werden soll, sondern wie ihre Nutzung gesteuert, gesichert und gelenkt werden kann, während gleichzeitig bestehende und neu auftretende Bedrohungen unter Kontrolle gehalten werden. Dieser Bericht zeigt, dass die Institutionen im Vergleich zur Geschwindigkeit der KI-Einführung bereits jetzt in Bezug auf wirksame Richtlinien, Governance und Budgetierung ins Hintertreffen geraten. Diese Verzögerungen bei Governance, Schulung und aktualisierten Sicherheitsmaßnahmen könnten sich in naher Zukunft als noch nachteiliger erweisen, da Bildungseinrichtungen bereits von KI-bedingten Bedrohungen und schädlichem Missbrauch berichten.

Die Daten legen drei zentrale Anforderungen für die heutigen Bildungsverantwortlichen nahe:

- **Schließen der Richtlinienlücke:** Formalisieren von KI-Richtlinien, die die Einführung mit einer verantwortungsvollen Nutzung in Einklang bringen.
- **Stärkung der Widerstandsfähigkeit:** Investition in Schulungen, Sensibilisierung, Cybersicherheit und Erkennungstools, um Mitarbeiter und Studenten besser auf KI-basierte Bedrohungen vorzubereiten.
- **Vertrauen schützen:** Direktes Adressieren von Datenschutz- und ethischen Bedenken sowie Sicherstellung von Maßnahmen zur Steuerung der KI-Nutzung, die das Vertrauen der Studierenden oder der Gemeinschaft nicht untergraben.

In der Praxis bedeutet dies, sofort umsetzbare Schritte zur Stärkung der Abwehr zu unternehmen:

- Erzwingen einer Multi-Faktor-Authentifizierung (MFA) auf allen Systemen, um das Risiko kompromittierter Konten zu verringern.
- Einführung einer Privileged Access Management (PAM)-Lösung, um zu kontrollieren, wer auf vertrauliche Daten und kritische Systeme zugreifen kann.
- Schulung von Mitarbeitern und Lernenden für den Umgang mit sicheren Passwörtern, um einen der häufigsten Einstiegspunkte für Angreifer zu reduzieren.
- Einsatz einer Echtzeiterkennung und -überwachung, um KI-gestütztes Phishing, Deepfakes und andere neue Bedrohungen zu erkennen, bevor sie eskalieren.
- Regelmäßiges Überprüfen und Aktualisieren der KI-Richtlinien, um sicherzustellen, dass sie mit neuen Technologien, Risiken und Anwendungsfällen im Klassenzimmer und Hörsaal Schritt halten.

Für Schulen und Universitäten werden die nächsten zwei Jahre entscheidend dafür sein, ob KI zu einem vertrauenswürdigen Partner in der Bildung wird oder eine anhaltende Schwachstelle darstellt. Durch diese proaktiven Schritte können Institutionen jetzt mit der Einführung Schritt halten und gleichzeitig der sich entwickelnden Bedrohungslandschaft einen Schritt voraus sein.

Methodologie

Keeper Security, ein Innovator im Bereich Cybersicherheit und Anbieter der führenden Zero-Trust und Zero-Knowledge Privileged Access Management (PAM)-Plattform, beauftragte das unabhängige Forschungsinstitut TrendCandy mit einer Umfrage unter 1.460 Bildungsadministratoren in den USA und Großbritannien zu der Frage, wie Schulen mit der Einführung, Nutzung und Cybersicherheitsbereitschaft von KI umgehen.

Die honorierte Online-Umfrage richtete sich an wichtige Führungskräfte von Bildungseinrichtungen in den USA und Großbritannien und erfüllte strenge Anforderungen an die Umfragemethodik, darunter Zufallsstichproben, Doppelblindverfahren und Datenqualitätskontrollen.

Die Fehlerspanne für diese Studie beträgt +/- 3 % bei einem Konfidenzniveau von 95 %.

Über Keeper Security

Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersicherheitsplattform von Keeper ist mit einer End-to-End-Verschlüsselung ausgestattet und genießt das Vertrauen von Fortune-100-Unternehmen, um jeden Benutzer auf jedem Gerät und an jedem Standort zu schützen. Unsere patentierte Zero-Trust- und Zero-Knowledge-Lösung für das Privileged Access Management vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriffen und Remote-Browser-Isolation. Durch die Kombination dieser wichtigen Identitäts- und Zugriffsverwaltungskomponenten in einer einzigen cloudbasierten Lösung bietet Keeper beispiellose Transparenz, Sicherheit und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Compliance- und Audit-Anforderungen. Erfahren Sie unter KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.