



Approfondimento

L'Intelligenza Artificiale a Scuola

**Safer Internet Day 2025:
tra AI Act, DeepSeek e
ChatGPT - Sicurezza
Digitale e Protezione
Digitale**

Approfondimento: **Safer Internet Day 2025: tra AI Act, DeepSeek e ChatGPT - Sicurezza Digitale e Protezione Digitale: Non è incubo, ma opportunità!**

Intelligenza artificiale a Scuola: sfida inevitabile o porta aperta sul futuro?

L'introduzione dell'**Intelligenza Artificiale** (IA) ha avuto un forte impatto sulle nostre vite quotidiane e lo stesso vale per il sistema scolastico italiano.

...DeepSeek? ChatGPT? AI Act europeo?

Fra telegiornali e i feed dei nostri social network, nomi come questi, per alcuni mai sentiti prima, nelle ultime settimane sembrano essere nella bocca di tutti, è normale sentirsi disorientati.

In un'altalena di entusiasmo verso le innovazioni e preoccupazioni per i potenziali rischi, trovare una bussola, una direzione chiara per orientarsi, può essere difficoltoso. Il **Safer Internet Day 2025** rappresenta una buona occasione per fare chiarezza in materia di sicurezza. **L'IA rappresenta davvero una minaccia per la nostra scuola o, piuttosto, una straordinaria opportunità da cogliere?**

Sicurezza e protezione digitali non sono ostacoli all'innovazione, ma strumenti per costruire un futuro scolastico più ricco e stimolante: una scuola "sicura" è in grado di sperimentare, crescere, preparare adeguatamente gli studenti per il mondo futuro. Siete pronti a trasformare questa "sfida" in "opportunità"?

IA, sicurezza e protezione digitale: elementi chiave per il futuro della scuola

Come si traduce concretamente questa visione nella scuola italiana, se vogliamo garantire un ambiente adeguato agli studenti?

La risposta sta nell'integrazione sinergica di due concetti: **Sicurezza Digitale (Safety)** e **Protezione Digitale (Security)**. Comprendere la distinzione e la complementarità di questi due aspetti è essenziale per sfruttare le potenzialità dell'Intelligenza Artificiale in ambito educativo in modo consapevole e responsabile.

- **Sicurezza Digitale (Safety)**, ovvero la sicurezza nell'utilizzo didattico dell'IA, consiste nel garantire che l'IA sia uno strumento positivo per l'apprendimento e per la crescita degli studenti, prevenendo rischi quali:
 - **Pregiudizi (BIAS):** modelli come DeepSeek - e i derivati diretti della versione R1- possono presentare pregiudizi introdotti più o meno involontariamente nei dati di addestramento o nella fase di allineamento, portando alla generazione di concetti inadatti o comportamenti problematici se utilizzati da allievi senza la supervisione di un adulto. Ad esempio, studi come quelli di Cisco su DeepSeek R1 evidenziano vulnerabilità problematiche in questo senso, mentre modelli come GPT-4o o Gemini sono generalmente più attenti alla *safety*, nonostante ci siano ancora ampi margini di miglioramento.

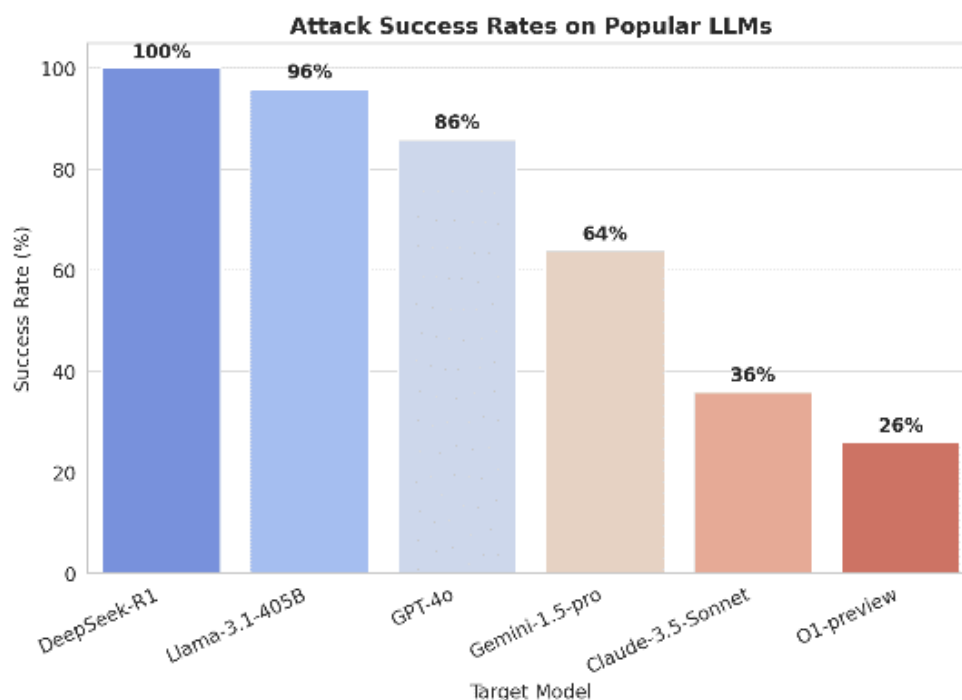


Figura 1: Questo grafico mostra quanto facilmente alcuni modelli di intelligenza artificiale possono essere "ingannati" da attacchi informatici. Un valore più alto indica una maggiore vulnerabilità, mentre un valore più basso significa che il modello resiste meglio

- **Disinformazione e verifica delle fonti:** l'IA generativa, quando viene usata in maniera impropria, è in grado di velocizzare la creazione di *deepfake* e *fake news*. È importante educare gli studenti al pensiero critico affinché imparino a valutare quanto le informazioni ricevute siano affidabili.
- **Gestione dei Dati Personali:** ogni attività didattica che prevede l'uso di strumenti di Intelligenza Artificiale - ma è in generale vero per tutte le piattaforme presenti in Rete - deve tutelare i dati personali degli studenti, rispettando il GDPR, minimizzando la raccolta di informazioni e adottando opportune misure di sicurezza.
- **Integrazione pedagogica dell'IA:** deve arricchire l'apprendimento e supportare l'inclusione, non ridursi a mero strumento tecnologico.
- **Protezione Digitale (Security),** ossia la *sicurezza dell'infrastruttura tecnologica*. Ogni docente, anche individualmente, nel suo piccolo, può contribuire a garantire:
 - **Infrastruttura digitale scolastica affidabile e sicura.** Docenti e studenti devono usare dispositivi e reti sicuri. La scuola deve selezionare fornitori qualificati e trasparenti per i servizi digitali, inclusi quelli che integrano l'IA, valutando attentamente affidabilità e serietà.
 - **Dati scolastici protetti.** Informazioni sensibili devono essere protette da accessi non autorizzati, attacchi e perdite, con comportamenti responsabili nella gestione delle credenziali e rispetto delle policy di sicurezza.
 - **Servizi digitali scolastici resilienti e disponibili.** Sistemi di gestione e piattaforme didattiche devono essere sempre operativi, protetti da interruzioni e problemi di cybersecurity. La collaborazione e la consapevolezza di ogni docente sono fondamentali per una scuola "cyber-resiliente".

In sintesi, *safety* e *security* sono pilastri per una scuola che integra l'IA in modo efficace, responsabile e inclusivo. Ogni insegnante, con il proprio impegno quotidiano, è protagonista di questa trasformazione positiva della scuola digitale italiana.

Problema: Rischio IA a Scuola (Spiegazione <i>non-tech</i>)	Opportunità: Trasformare il rischio in forza	Soluzioni pratiche per insegnanti
Rischio Privacy Dati Studenti (Se usi IA online non sicura, dati ragazzi = rischio)	Tutela Dati Studenti: Scuola Modello Privacy-First	<ul style="list-style-type: none"> • Verificare la privacy policy: leggere <i>attentamente</i> le norme sulla privacy dello strumento IA. Sono chiare e <i>facilmente comprensibili</i>? Tutela davvero i dati dei minori? • Controllare la Conformità GDPR: accertarsi che lo strumento dichiari <i>esplicitamente</i> la conformità al GDPR (Regolamento Europeo Privacy). Cercare <i>loghi</i> o <i>certificazioni</i> di enti terzi. • Sensibilizzare gli Studenti alla Privacy: educare i ragazzi in modo <i>concreto</i>: perché proteggere i dati online è importante <i>anche a scuola</i>? (Esempio: non condividere dati personali sensibili in chat IA non verificate o aperte al pubblico)
Cyber-Vigilanza - Phishing AI-Powered (Mail false con IA = truffe online ancora più difficili da smascherare)	Scuola Protetta "Cyber-Vigilante"	<ul style="list-style-type: none"> • Aggiornare le conoscenze Anti-Phishing: partecipare a brevi corsi online o consultare guide aggiornate sul phishing "potenziato" dall'IA. Essere preparati è la miglior difesa! • Verificare SEMPRE l'Autenticità delle E-mail: non fidarsi dell'apparenza! Controllare sempre attentamente l'indirizzo e-mail completo del mittente. È davvero quello che ci si aspetta?

		<ul style="list-style-type: none"> • Segnalare ogni dubbio al Supporto Tecnico (e NON Cliccare!): E-mail sospetta o insolita? Non aprire link o allegati! Eventualmente segnalare all'ufficio tecnico scolastico e chiedere sempre una verifica prima di agire.
<p>AI-Literacy - Disinformazione Online (Fake News IA) (IA crea notizie false così realistiche = quasi impossibile distinguerle dalle vere "a occhio nudo")</p>	<p>Scuola Informata e Resiliente all'IA</p>	<ul style="list-style-type: none"> • Insegnare metodi di verifica delle fonti (pensiero critico al centro): spiegare <i>metodologie pratiche</i> per valutare l'attendibilità delle fonti online e smascherare la disinformazione. (Esempio: "le 5 W" del giornalismo, fact-checking incrociato su più fonti, verifica autorevolezza sito web) • Analizzare esempi di contenuti FAKE IA (imparare dagli errori): utilizzare in classe esempi reali e recenti di <i>deepfake</i> (video manipolati) o <i>fake news</i> generate con IA, de-costruendoli insieme agli studenti per capire le tecniche di inganno e i segnali di allarme. • Promuovere fonti affidabili (costruire una "bussola"): creare insieme agli studenti una lista condivisa e "dinamica" di siti web e testate giornalistiche riconosciute per la loro accuratezza, verificabilità delle fonti e deontologia professionale nell'informazione.

<p>Scelta consapevole - Strumenti non affidabili (App IA non tutte OK per scuola. Errore di scelta = problemi seri per privacy e sicurezza)</p>	<p>Scuola Cyber - Resiliente Scelte tecnologiche consapevoli</p>	<ul style="list-style-type: none"> • Valutare attentamente le opzioni software (Utilità e Sicurezza): prima di adottare <i>qualsiasi</i> nuovo strumento digitale (specie se basato su IA), valutarne con <i>rigore</i> la reale utilità didattica, la sua <i>effettiva</i> adeguatezza al contesto scolastico e, <i>soprattutto</i>, le garanzie di sicurezza e privacy che offre. Non basarsi <i>mai</i> solo su criteri superficiali come "gratuità" o "facilità d'uso". • Analizzare a fondo Privacy Policy e Termini di Servizio (Non fermarsi alla superficie): dedicare il tempo necessario a <i>leggere e comprendere a fondo</i>, punto per punto, le "regole sulla privacy" (Privacy Policy) e le "condizioni d'uso" (Termini di Servizio) dello strumento. Valutare con <i>spirito critico</i> e senza fretta le modalità di trattamento dei dati, le clausole contrattuali e le garanzie reali offerte dal fornitore. • Privilegiare fornitori qualificati e affidabili (Reputazione = Affidabilità): nelle scelte tecnologiche per la scuola, orientarsi <i>sempre</i> verso aziende e fornitori <i>riconosciuti nel settore per la serietà, la trasparenza, la solidità finanziaria e, in particolare, per la comprovata attenzione alla sicurezza digitale e alla protezione dei dati</i>. La reputazione del fornitore, le certificazioni di sicurezza che possiede e le referenze di altre scuole che utilizzano i suoi prodotti sono indicatori di affidabilità importanti.
--	--	---

IA a Scuola: non incubo, ma progetto di futuro. Insieme. Con la "bussola" dell'AI Act.

Il **Safer Internet Day 2025** è un invito a formarci per poter creare un ambiente digitale sicuro per gli studenti, che possa prepararli all'uso responsabile dell'Intelligenza Artificiale.

Questo è particolarmente importante poiché il **2 febbraio 2025** sono divenuti operativi alcuni divieti relativi ai sistemi considerati ad alto rischio previsti dall'**AI Act** (regolamento sull'intelligenza artificiale, mira a disciplinare l'uso dei sistemi di intelligenza artificiale nell'Unione Europea). Possiamo affrontare questa sfida vedendo l'IA come un'**opportunità per migliorare l'educazione, promuovere l'inclusione e formare cittadini digitali consapevoli**.

Investire in Sicurezza Digitale (*Safety*) e Protezione Digitale (*Security*) è il prerequisito per costruire una scuola cyber-resiliente e orientata alla tutela della Privacy.

Le opportunità sono concrete: diventare un esempio nella Tutela della Privacy, promuovere una Cyber-Vigilanza Educativa, sviluppare una AI-Literacy diffusa e fare Scelte Tecnologiche Consapevoli e Responsabili.

Ci troviamo in un momento di svolta per il futuro digitale della scuola italiana. Non si tratta semplicemente di adottare nuove tecnologie, ma di intraprendere un viaggio collettivo di trasformazione consapevole.

L'AI Act ci offre una bussola anche etica per navigare questo territorio inesplorato, ma sta a noi - docenti, dirigenti, famiglie e stakeholder - dare forma a una visione condivisa, in linea con i nostri valori e principi. È una sfida ambiziosa, ma anche un'opportunità straordinaria per ridisegnare insieme il futuro dell'educazione.

AI Act europeo - principali divieti operativi a partire dal 2 febbraio 2025 di interesse per le comunità scolastiche:

- Sistemi IA manipolativi
- Sorveglianza biometrica indiscriminata
- Riconoscimento delle emozioni iniquo
- Categorizzazione biometrica discriminatoria
- Social Scoring lesivo della dignità

Fonti

- European AI ACT - [Regolamento - UE - 2024/1689 - EN - EUR-Lex](#)
- Safer Internet Day 2025 - [BETTER INTERNET FOR KIDS - Safer Internet Day 2025](#)
- [5 Key Cyber Security Trends for 2025 - Check Point Blog](#)
- IBM Technology: Cybersecurity Trends for 2025 - [Cybersecurity Trends for 2025 and Beyond](#)
- Evaluating Security Risk in DeepSeek - [Evaluating Security Risk in DeepSeek - Cisco Blogs](#)
- [Predicting the Future Cybersecurity Threats with the Greatest Potential for Disruption - Top Cybersecurity Trend Predictions for 2025+... | BeyondTrust](#)
- Global Cybersecurity Outlook 2025 - [Global Cybersecurity Outlook 2025 | World Economic Forum](#)