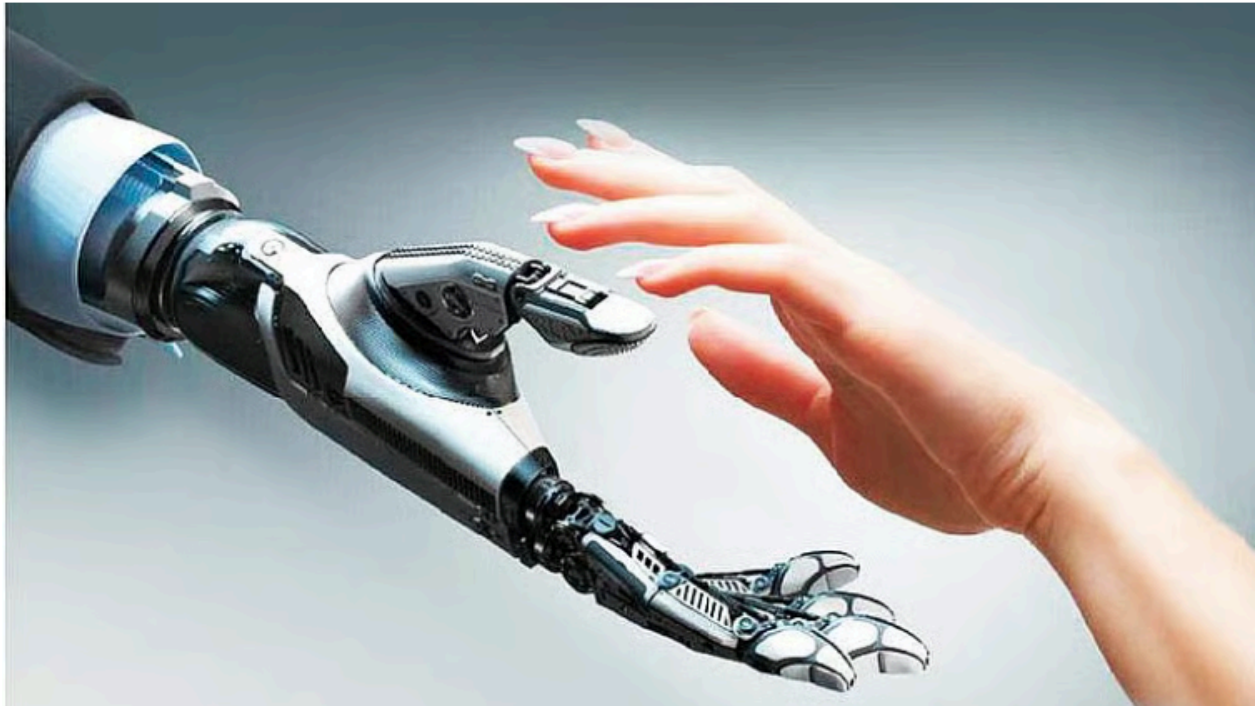


The new Digital divide: AI use vs AI safety

The students best prepared for an AI-driven future will be those who understand its capabilities, limitations and risks well enough to use it responsibly



In an exclusive interview with EdexLive, Harish Kumar, Chief Executive Officer of Quick Heal Technologies, discusses various aspects related to the use of artificial intelligence and the risks which accompany AI usage.

The first digital divide was largely about access: who had an internet connection, a smartphone or a computer, and who did not. In the age of artificial intelligence, however, the divide could be between students who know how to use AI critically and safely and those who can access powerful AI tools but lack the judgment to navigate the risks that come with them.

For students, AI should be viewed as a thinking partner rather than a replacement for thinking. "For college students and young adults, AI should be taught as a thinking partner, not a thinking replacement," said Harish Kumar, Chief Executive Officer of Quick Heal Technologies. "Students should first learn to frame a problem, develop their own point of view, and then use AI to refine research, test arguments, or explore alternate perspectives." He added that this

balance is particularly important in higher education, where independent thinking, originality and judgment matter as much as speed.

As AI makes online interactions more convincing, students are exposed to cyber risks that can be difficult to identify. “For students, the danger is no longer limited to harmful content but extends to credibility manipulation, where a fake classmate, professor, recruiter, or support channel appears authentic” according to Kumar. “Attackers are increasingly able to mimic writing styles, speech patterns, and even video presence, while campaigns such as fake job and recruiter scams show how trust can be weaponized against young people.”

The changing nature of these threats is also altering how people perceive online trust. Earlier, users could sometimes identify scams through obvious warning signs such as poor grammar or awkward imitation. AI can now generate polished messages, realistic conversations and convincing digital identities, making malicious interactions appear far more authentic.

For students, this means that something looking genuine online can no longer be considered sufficient proof of authenticity. Verification must become a habit. Checking URLs carefully, avoiding unofficial app links and confirming suspicious requests through a second communication channel can help students avoid increasingly sophisticated deception.

According to Kumar, digital safety needs to become part of the wider educational experience—from college orientation and classroom research to placement training, digital payments, collaboration platforms and everyday app usage. Public-private partnerships could play an important role in making such education relevant. "Government can provide policy direction, guardrails, and curriculum standards, while industry players such as Quick Heal can contribute real-world threat intelligence, awareness modules, phishing and scam education, fake-app detection guidance, and practical digital-safety training that reflects what students actually face online today," Kumar said.