The Indian EXPRESS

When paradise doesn't exist: AI-powered deepfake holidays are the new travel trap; here's how to avoid them

AI-generated resorts and experiences are luring travellers worldwide, and experts warn India could be next. Here's how to spot the red flags before you book.

Written by **Swarupa Tripathy**
New Delhi | October 1, 2025 06:31 PM IST

Modern deepfake travel scams go far beyond Photoshop. (Source: Freepik)

Imagine scrolling through Instagram and spotting a breathtaking video of a Maldives resort — crystal-clear waters, luxurious overwater villas, all for just Rs 5,000. The influencer testimonial feels genuine, the website appears professional, and the comments are overwhelmingly positive. You book instantly, only to discover later that this paradise never existed. Welcome to travel's new frontier of fraud: AI-generated deepfake destinations.

This is no distant threat. Globally, many have **fallen victim to such scams**. A report by *The Independent* recounted the story of a Malaysian couple who travelled across the country for a cable car ride, only to discover that everything was AI-generated. The fake "Kuak Skyride" featured queues, tourists taking photos, a lavish meal, and a deer petting zoo — all fabricated by AI.

Closer home, actor Archana Puran Singh revealed her family lost money in Dubai after booking an indoor skydiving session on a fake website. "We've already paid, and the tickets weren't cheap. Dubai mein humare paise doob gaye" (We lost money in Dubai), she said.

In 2024, the *BBC* reported that Booking.com warned of an explosion in travel scams driven by AI, with online threats surging 500–900 per cent over 18 months. Phishing and fake listings are spiking alongside generative AI tools like ChatGPT.

This trend is already visible globally, and it's only a matter of time before India experiences a similar surge, making it crucial to be aware of what to watch out for.

The perfect digital deception

Modern deepfake travel scams go far beyond Photoshop. Jaspreet Bindra, CEO of AI&Beyond, said, "With GenAI, it has never been easier to fabricate convincing destinations. Tools like Stable Diffusion, Midjourney, Runway, and open-source video generators create **hyper-realistic images and clips** of beaches, mountains, or forests that do not exist."

Sneha Katkar, head of product strategy at Quick Heal Technologies, a cybersecurity platform, said, "Deepfake travel scams combine generative-AI imagery with social-engineering precision. AI-voiced 'travel vloggers' praise resorts that never existed. Unlike old Photoshop jobs, these ultra-high-resolution clips survive reverse-image searches and even trick automated ad-platform vetting."

Dikshant Dave, CEO of Zigment, noted the accessibility: "Anyone with advanced generative AI tools can now create hyper-realistic videos of non-existent places. What once required professional studios can now be done by hobbyists."

The psychology of travel dreams

Why do we fall for these fakes? Humans are naturally drawn to exotic, aspirational content. "Travel content taps into emotion and aspiration. Coupled with urgency-driven marketing, people suspend scepticism. The 'wishful thinking bias' is strong in travel," said Dave.

Ankush Sabharwal, CEO and founder of CoRover.ai, said that the brain trusts novel or aspirational content. "The romanticism of 'discovering hidden treasures' or 'uncovering paradise' pulls on our psychological strings of newness, social proof, and FOMO," he said.

Bindra noted that social media amplifies these vulnerabilities, with likes and shares rewarding instant belief rather than careful scepticism. "Add the 'trust halo' of influencers or official-looking accounts, and fabricated travel videos can spread virally before doubts set in," Bindra said.

What about India?

India's digital boom and growing disposable income make it a target. Amit Jaju, senior managing director at Ankura Consulting, warned: "First-time online users may not recognise these

scams. Budget travel is popular, and scammers take advantage of it. Apps like WhatsApp make it easy to spread fake offers quickly, especially in regional languages."

Katkar highlights India's high mobile usage and social-media engagement, saying, "Budget travellers rely on third-party aggregators and peer-recommendation videos. Deepfakes in vernacular languages widen the attack surface, with auto-translations tailored to Hindi, Tamil, or Marathi."

Katkar pointed to specific vulnerabilities, such as India's high mobile usage and social media engagement. "Budget travellers rely on third-party aggregators and peer-recommendation videos. Deepfakes in vernacular languages widen the attack surface, with auto-translations tailored to Hindi, Tamil, or Marathi," he said.

How the scam works

The technical execution of these scams is surprisingly sophisticated. Jaju broke down the process: "It usually starts with a fake website or social media page, sometimes cloned from a real agency. They might use stolen images or AI-generated videos to build trust. Payment is the next step; they'll often push you to pay via wallets or sketchy links. Once that's done, they vanish. Some even use AI voices to run fake customer service lines."

Katkar provided more technical detail, revealing that a typical campaign begins with "domain spoofing, such as 'goa-bliss-stay.in', backed by cloned payment APIs that silently redirect funds to crypto wallets." While deepfake videos seed credibility on social media, stolen KYC documents, bought off dark-web dumps, populate testimonial carousels. When a traveller clicks 'Book Now,' a fake gateway skims card data while generating a PDF 'e-ticket.'

The industry is taking notice. Ravi Gosain, president of IATO (Indian Association of Tour Operators), confirmed, "The last few months have brought about the threat of fake travel listings, alongside the use of altered photos and deceptive promotional videos to target travellers. Even as numerous sites attempt to fortify their authentication systems, scammers make use of AI tools."

IATO, along with its member agencies, implements rigorous verification measures to validate destination packages, accommodations, and tour offerings, Gosain said, adding, "Our procedures insist on in-house evaluations, partnerships with official tourism authorities, and proper accreditation of member agencies." Yet, the advanced capabilities of AI-generated forgeries require more robust partnerships.

Red flags to watch for

So how can travellers protect themselves? Experts offer **several key warning signs** to watch for.

Jaju suggested, “If it looks too good to be true, like a luxury Maldives package for Rs 5,000, it probably is. Also, check the reviews. Real ones tend to vary in tone and detail; fake ones sound oddly perfect or repetitive. And always verify the company’s contact details. If there’s no real address or the website was just created recently, that’s a red flag. Also, such videos do not have the influencer visit these destinations, but they use stock videos of the destinations.”

Katkar advocated for verification over aesthetics. He believes travellers need to “lean more towards provenance instead of aesthetics.” Cross-check new destinations against official tourism boards, validate hotel addresses on open maps, and scrutinise booking domains for misspelt HTTPS certificates. Abrupt payment requests via unfamiliar gateways or wallets are some key red flags to look out for, stresses Katkar.

Some travellers are cautious

Not all travellers are falling victim to these elaborate schemes. Pravar Anand, a travel enthusiast, shared his cautious approach. “I mostly trust authentic websites for travel information rather than being influenced by visuals or recommendations. While photos and videos can be attractive, they can also be edited or enhanced, so I don’t rely on them entirely. Reviews from official sources or verified platforms give me more confidence in making decisions,” he told indianexpress.com.

Anand’s verification process is thorough, involving cross-checking a deal on multiple websites before making any booking decision. This helps him understand if the pricing and offers are consistent across platforms. Additionally, he says that he looks for verified reviews and ratings to make sure the deal is genuine.

However, Anand acknowledged the limitations of current protection systems. “As of now, I don’t think there are any proper systems in place to help victims of deepfakes or fake AI destinations. Such an experience would definitely shake my trust and make me even more cautious in the future.”

What the future looks like

Combating deepfake travel scams requires a multi-pronged approach: stronger AI detection tools, public awareness campaigns, faster takedowns, tighter payment monitoring, and **regulations around AI-generated content**.

Sabharwal predicts real-time verification tools will soon allow travellers to authenticate photos and videos instantly, much like spam filters protect users today.

Until robust AI detection systems are widespread, the oldest rule of travel still applies: if it looks too good to be true, it probably is.