Maha Kumbh Mela 2025: Tips to prevent digital scams during the festival

The Maha Kumbh Mela is a once-in-a-lifetime spiritual journey for many, but staying vigilant is essential to ensure a safe experience.

By Anshul _January 13, 2025, 10:40:20 AM IST (Published)
3 Min Read

The Maha Kumbh Mela, a grand spiritual event held every 12 years, began on Monday (January 13) in Prayagraj. This gathering brings together millions of devotees seeking divine blessings. However, such massive gatherings may also attract fraudsters looking to exploit unsuspecting visitors.

From digital scams to accommodation frauds, here’s a look at the potential risks and how attendees can stay protected.

Common scams that can take place at Maha Kumbh Mela

Fake QR codes and digital payment fraud

With the widespread use of UPI and QR code payments, scammers may exploit devotees by distributing fake QR codes. Fraudulent donation links and unauthorised payment requests are also potential risks.

Amit Kumar, CTO of Easebuzz, explains, “Fraudsters may trick people into transferring money through bogus codes and links. Verifying QR codes before making payments and avoiding unsolicited offers is critical.”

Fake accommodation and travel listings

Scammers may create websites or ads promoting accommodations, flights, and tents that don’t exist. Victims could be asked to pay in advance, only to realize the service was a hoax.

Dhiraj Gupta, Co-founder of mFilterIT, warns, “Fraudsters use WhatsApp, emails, or fake websites to lure people with attractive deals. Once the payment is made, they disappear.”

Phishing and cyber attacks on public platforms

Large public systems like registration portals and booking websites may be targeted by cybercriminals.

Phishing emails and fake UPI payment requests are common tactics to trick individuals into revealing sensitive information.

Animesh Jha, VP of Wibmo, notes, “Denial-of-service (DoS) attacks on public platforms and fake links are frequent. Individuals must remain cautious while using these services.”

Public wi-fi risks

Scammers may exploit unsecured public Wi-Fi networks to steal personal data or hack devices.

Surveillance systems connected to default IPs could also be vulnerable to misuse.

Vishal Salvi, CEO of Quick Heal Technologies, states, “Public Wi-Fi and IP-based cameras are at risk of snooping. Cybercriminals can misuse these to access sensitive information.”

Book through verified platforms

Always use official government websites or trusted travel platforms like IRCTC for bookings.

Double-check URLs for secure gateways (look for “https://”) to avoid phishing websites.

Verify payment links and QR codes

Avoid scanning QR codes from unknown sources. Verify codes before making payments, and refrain from clicking on unsolicited donation links or payment requests.

Avoid public Wi-Fi

Use mobile data or a Virtual Private Network (VPN) for secure internet access. Avoid public Wi-Fi for any financial transactions or personal logins.

Stay informed through official apps

Download the Maha Kumbh Police App for regular updates on scams and security measures. Check for verified news and alerts to stay ahead of potential threats.

Report suspicious activities

If you come across fraudulent websites, apps, or social media accounts, inform local authorities or use the official grievance platforms to report them.

Solutions for added security

Quick Heal Technologies has launched its AntiFraud.AI solution to help safeguard against scams.

“We are offering a free three-month trial of our app during the festival to help devotees protect themselves from frauds,” says Salvi.

Easebuzz emphasises enabling two-factor authentication on payment apps to add an extra layer of security.

“Awareness is the first step to safety,” says Kumar.

mFilterIT suggests deploying AI-powered solutions to detect and counter scams proactively, urging devotees to cross-check details before making any payments.