ET Edge INSIGHTS

Inside Bihar’s online scam surge: How the state became a scammer’s playground, who’s targeting and why

On a busy morning in a small Bihar town, a tea seller accepts payments with a QR code taped to his stall. Nearby, a college student scrolls through WhatsApp messages about admissions, while a parent waits anxiously for a bank alert confirming a UPI transfer. This is the new digital Bihar—fast, connected, ambitious. And for cybercriminals, it has become fertile ground.

Quick Heal Technologies Limited, a global provider of cybersecurity solutions, has raised serious concern over the explosive rise in online scams hitting Bihar. According to researchers at Seqrite Labs, India’s largest malware analysis facility, scammers are deliberately exploiting three converging factors in the state: booming UPI usage, widespread QR-code adoption at local shops, and a large population of students and first-time digital users.

What the data shows

Findings from the India Cyber Threat Report 2026 by Seqrite Labs reveal that social engineering attacks phishing, vishing and smishing remain the most dominant threat vector in India, accounting for the highest volume of cyber incidents nationwide. The report also notes that signature-based malware detections crossed 415 million nationally, underlining the sheer scale at which malicious activity is operating

Crucially, states with rapid digital adoption but lower cybersecurity maturity show higher exposure to fraud, especially UPI-linked scams and impersonation attacks a pattern that mirrors Bihar's experience. Seqrite Labs processes over 1 million new malware samples daily and classifies nearly 600 million URLs, many of which are linked to phishing pages and fake financial apps targeting Indian users.

How scammers exploit Bihar's digital shift

Researchers at Seqrite Labs highlight that fraudsters thrive on Bihar's fast shift to apps and instant money movement. WhatsApp is flooded with messages claiming lottery wins, instant loans, or hacked family profiles begging for urgent cash. Fake college admission forms, leaked exam papers and work-from-home offers lure students into paying small "registration fees" that disappear instantly.

Cybercrime cases have surged as digital life takes over from UPI payments in small towns to online classes across districts—while low awareness leaves families, elders and youth exposed to classic traps like *"KYC update noW or your account Will be blocked"*, bogus job fees, and QR codes that debit accounts instead of crediting them.

Recent busts, as noted by Seqrite Labs, show a sharp rise in emotional manipulation scams, including deepfake audio/video of relatives in distress and authority scams where fake bank representatives push victims to install remote access apps. Many rural cases go unreported, allowing criminal networks to scale rapidly via Telegram channels and social media groups promising guaranteed seats or high-paying jobs.

Who is most at risk

Quick Heal Technologies Limited warns that busy parents, curious children, and job-hunting freshers are the most commonly targeted groups. Along with Bihar’s large youth population is a prime target. Scammers lure students with fake college admission forms, leaked exam papers, work-from-home offers and job postings promising high salaries. A small “registration fee” or “security deposit” is demanded and once paid, the fraudsters vanish.

WhatsApp and Telegram groups amplify the damage, spreading false promises of guaranteed seats or quick employment. With limited reporting from rural areas, these scams often go unchecked, allowing criminal networks to scale rapidly.

Curiosity, urgency and trust in “official-looking” messages continue to fuel these attacks. The India Cyber Threat Report 2026 also flags AI-driven and impersonation-based attacks as a growing trend, making scams harder to detect for first-time users.

Recent cases uncovered by Seqrite Labs reveal a worrying shift toward emotional manipulation. Victims receive calls from fake bank officials urging them to install remote access apps. Others are targeted with deepfake audio or video of “relatives” claiming to be in trouble and urgently asking for money.

Lottery wins, instant loan offers, hacked family accounts begging for help these scams thrive on fear, greed and empathy. As digital life deepens across cities like Gaya and Bhagalpur, so do these sophisticated tricks.

Simple habits, strong defence

To counter this growing threat, Quick Heal Technologies Limited advises users to follow basic but critical rules:

- Never share OTPs, PINs or screen access
- Verify links only via official apps or by typing websites manually
- Avoid scanning unknown QR codes

- Report suspected fraud immediately to 1930 or cybercrime.gov.in with screenshots and transaction IDs to help freeze funds quickly

Families and students are encouraged to use strong, unique passwords with multi-factor authentication, openly discuss pressure tactics and "too-good-to-be-true" offers, set parental controls on children's devices, and download apps only from trusted stores. Seqrite Labs researchers also recommend checking seller reviews, ignoring fake "parcel hold" fees, and avoiding random links sent over SMS or WhatsApp key steps in defending against impersonation, romance scams and delivery frauds affecting cities like Gaya and Bhagalpur.

The road ahead

Bihar's digital transformation is irreversible and that is undeniably a positive shift. From financial inclusion to education and employment access, technology has opened doors at an unprecedented scale. Yet, without awareness and protection, the same progress can be twisted into an advantage for cybercriminals who thrive on the gap between technology and trust. The choice facing users is stark: remain vulnerable or become vigilant.

As researchers at Seqrite Labs emphasise, cybersecurity today is no longer just about securing devices or networks it is fundamentally about securing people. In a state accelerating toward a digital-first future, awareness, caution and informed behaviour have emerged as the strongest lines of defence.

For Bihar and for India at large the message is unambiguous. Digital progress cannot and should not be rolled back, but without vigilance, it can be weaponised. By combining data-backed threat intelligence from Seqrite Labs, responsible digital habits, and advanced protection solutions from Quick Heal Technologies Limited, users can shift the balance of power—transforming Bihar from a scammer's playground into a benchmark for digital resilience and cyber confidence.