Cybercrime & Fraud · 5 Min Read

Fake Traffic Challan scam: How cybercriminals are exploiting India's digital trust

Cybercriminals are exploiting India's digital governance by sending fake traffic challan messages via WhatsApp, tricking vehicle owners into downloading malicious APKs. These apps grant attackers full device control, stealing sensitive data. Authorities emphasize that government agencies do not send such demands through WhatsApp, urging vigilance and independent verification.

Govind Rammurthy • ETCISO
Published On May 1, 2026 at 08:00 AM IST

As India rapidly embraces digital governance, cybercriminals are finding new ways to exploit this trust. A recent fraud alert from Odisha highlights a growing scam where unsuspecting vehicle owners receive fake traffic challan messages designed to steal sensitive data and compromise their devices.

The scam operates with elegant simplicity. A WhatsApp message arrives from a number claiming to be "M Parivahan," informing vehicle owners they violated traffic rules and must pay a ₹2,200 fine. The message includes the vehicle number - lending false credibility - and asks users to download an "official app" to process payment. That downloaded APK file is where the scam converts from nuisance to disaster.

According to cyber experts, once installed, the malicious APK grants attackers control over the victim's mobile device. Gallery data, banking credentials, contact lists, WhatsApp messages - everything becomes accessible to criminals who can monitor, exfiltrate, or misuse

information in countless ways. An Odisha woman who received such a message avoided becoming a victim through basic common sense: her vehicle had been parked at home for days, making a red-light violation physically impossible.

What makes this scam particularly effective is its exploitation of government digitalization initiatives. India has legitimately moved many services online - vehicle registration, driving license renewals, traffic fine payments - training citizens to expect government communications through digital channels. Scammers exploit this learned behavior, impersonating legitimate services that genuinely do exist, making fake messages harder to distinguish from authentic ones without careful examination.

Bhubaneswar Cyber Police Assistant Commissioner Suchismita Das clarified that no messages or links related to traffic challans are sent via WhatsApp to vehicle owners, which should be widely known but evidently isn't. The official clarification highlights a broader problem: citizens need clear, authoritative information about how the government actually communicates versus how scammers pretend the government communicates, and that information needs distribution through channels citizens actually use.

The scale of the problem is substantial. Odisha registered 2,803 cybercrime cases in 2025. According to Chief Minister Mohan Charan Majhi's statement in the Assembly, between June 2024 and December 2025, fraud worth ₹260.61 crore was reported, with only ₹61.36 lakh refunded to the victim - a recovery rate of less than 0.25%. These statistics demonstrate why prevention matters more than recovery: once money transfers to criminal accounts, getting it back proves extremely difficult regardless of law enforcement effort.

The technical defense against APK-based scams requires security software that can scan downloaded files before installation, identify malicious code patterns, and block execution before damage occurs. CERT-In, as part of its Swachh Bharat Abhiyan digital hygiene initiative, lists eScan as the only provider of a free botnet detection and removal tool for Android devices - particularly relevant given that mobile phones are the primary target for these WhatsApp-based scams.

The Odisha cyber expert's advice to "install tools like eScan or eScan bot removal from the Play Store to detect and remove malicious APK files" underscores the practical reality that many users need automated protection because they may not recognize threats themselves. But technology alone cannot solve problems rooted in human behavior and

trust exploitation.

The prevention advice remains frustratingly simple yet frequently ignored. Never download applications from links sent via WhatsApp or SMS, regardless of how official they appear. Never install APK files from unknown sources - legitimate apps come from Google Play Store or official websites accessed by typing URLs directly rather than clicking links. When you receive unexpected fines or payment demands, verify them by contacting the organization through official channels rather than responding to the message itself.

The "close the tab and start over" principle applies here: if you receive a traffic challan message and want to verify whether it's legitimate, ignore the message entirely and check the official Parivahan or state transport website by typing the URL yourself. If a genuine challan exists, it will appear in your official records. If nothing appears, the message was fake. This takes three minutes and completely defeats the scam's urgency-based pressure tactics.

What's particularly frustrating about these scams is their preventability. Unlike sophisticated zero-day exploits requiring advanced security expertise, fake challan scams succeed through basic social engineering that common sense should defeat. Yet they work repeatedly, generating enough revenue to justify continued operation, which means either common sense isn't as common as we assume or urgency and fear override rational thinking when people see unexpected government communications demanding payment.

The cybersecurity industry can provide tools - malware scanners, threat detection, secure browsers, and endpoint protection - but cannot install skepticism or patience, which remain the most effective defenses against social engineering attacks. The Odisha woman who avoided the scam didn't use sophisticated security software; she used common sense thinking by questioning whether a red-light violation made sense given her vehicle's location. That simple pause prevented disaster.

Cyber Police can arrest attackers, which they're doing - 744 arrests in Odisha during 2025 - but arrests don't prevent scams; they just punish unsuccessful scammers after victims already suffer losses. Real prevention requires widespread awareness that government agencies don't send payment links via WhatsApp, unexpected demands for urgent action usually indicate scams rather than legitimate communications, and three minutes of verification beats hours of recovery effort.

The fake challan scam will evolve as defenses improve. Attackers will find new impersonation targets, craft more convincing messages, and exploit different trust relationships. But the fundamental defense remains constant: verify independently, never click links in unexpected messages, and when something feels wrong, trust that instinct over any claimed urgency. Technology provides tools, but skepticism remains irreplaceable.

The author is Govind Rammurthy, CEO & Managing Director of eScan,