Telangana emerges a key target for hackers: Seqrite report

Updated - February 24, 2025 at 07:28 PM. | Hyderabad

Targets include Telangana Govt portal, Dy CM’s office

BY K V KURMANATH

With several growing economic hubs in the State, people also fell prey to nearly 26,000 business and investment scams. | Photo Credit: thomaguery

Telangana has become a key target for hackers with 23 per cent of all malware detected in the country in 2024 were reported in the State.

Seqrite, a cybersecurity company, said that the State reported 6.25 million incidents last year. The enterprise solutions arm of the cybersecurity company Quick Heal released the Telangana Cyber Threat Report 2025, which reported a dramatic escalation in cyber threats in key sectors such as healthcare, education, and government institutions.

The report reveals that identity theft is the most reported cybercrime in the State, with nearly 30,000 incidents registered last year.

“This includes 11,125 cases of unauthorised transactions, and 5,369 incidents of KYC (know your customer) updation fraud. Impersonation frauds accounted for 18,647 cases, which included courier frauds, police impersonation and digital arrest scams,” the report said.

With several growing economic hubs in the State, people also fell prey to nearly 26,000 business and investment scams. Advertisement fraud (17,669 cases) and loan fraud (12,589 cases) comprised other prominent forms of fraud detected in the State.

Seqrite said the year also saw a sharp rise in ransomware attacks. “The State witnessed an average of 47 daily attacks and 17,505 incidents last year. T/ITES, manufacturing, and education were among the top sectors that were targetted and reported disruptions due to cyberattacks,” it said.

Hacktivist groups operating through platforms like Telegram have also intensified their activities in the State. These groups have targeted government portals such as data.telangana.gov.in and educational institutions like the Jawaharlal Nehru Architecture and Fine Arts University.

“Sensitive citizen data, login credentials, and governmental documents were leaked online, while website defacements tarnished the reputations of public institutions. For instance, the Deputy Chief Minister’s website was breached, exposing internal documents that raised serious concerns about data privacy and security,” the report said.