CIO&LEADER

Shoulder Surfing and Human-Targeted Attacks Still Outpacing Technology-Based Threats in India, Warns Seqrite

Seqrite, the enterprise security arm of Quick Heal Technologies Limited, a global provider of cybersecurity solutions, today cautioned organisations and citizens that human-targeted attacks – including shoulder surfing, phishing, vishing, smishing, impersonation and digital honey traps – continue to outpace purely technology-led threats in India. While attacks are becoming more automated and AI-assisted, the most successful campaigns still begin by exploiting a person's trust, attention, fear or routine behaviour.

Seqrite's India Cyber Threat Report 2026 found that social engineering remains the top attack vector reported by organisations, ahead of malware and web-application attacks. The findings underline a persistent reality: sophisticated security technologies can be undermined when an attacker persuades an employee to disclose information, scan a malicious QR code, approve a login prompt, share an OTP, install a fake app or open a deceptive attachment.

"Shoulder surfing" is one of the most overlooked examples of this human-centric threat landscape. In offices, airports, co-working spaces, cafés, bank branches and public transport, attackers or opportunistic observers can watch users enter PINs, passwords, UPI credentials or confidential information on their devices. Even small fragments of information – an employee ID, a one-time password, a meeting subject line, a tax document or a visible screen notification – can be combined with public data and social engineering to build a convincing fraud or intrusion attempt.

Seqrite's analysis also identified a rise in human-focused campaigns that operate without relying on traditional malware at the outset. Digital honey traps, for example, use AI-generated profiles, realistic photographs and crafted personal conversations on social media, dating platforms and messaging apps to establish trust before seeking workplace information, internal documents or private content. In observed cases, victims were later exposed to blackmail or coercion after sharing sensitive information.

Similarly, attackers are exploiting the familiarity of public services, brands and everyday transactions. The report documents fake government-service apps and websites that mimic trusted interfaces, including traffic-challan and High-Security Registration Plate services, to harvest OTPs, payment details, personal identifiers and device permissions. Fraudsters use urgency-driven language such as "final notice," "fine imposed" or "account blocked" to override caution and force immediate action.

While technology remains essential, it must reinforce human judgement rather than assume it. Seqrite advises organisations to adopt layered security that integrates endpoint protection, identity monitoring, email and web controls, threat intelligence and behavioural analytics. The

report found that behaviour-based security technologies, including next-generation antivirus and anti-ransomware engines, identified more than 34 million anomalous detections during the reporting period, highlighting the value of detecting suspicious activity that may evade traditional signatures.

Seqrite urges organisations to strengthen the human layer of cybersecurity through continuous awareness programmes, phishing and vishing simulations, role-based training, phishing-resistant multi-factor authentication and behaviour-driven access policies. Employees should be encouraged to challenge unexpected requests, independently verify the identity of callers and senders, and report suspicious activity without fear of blame. Clear-screen practices, privacy filters, device-locking discipline and caution while entering credentials in public spaces can also reduce exposure to shoulder-surfing risks. Advanced, AI-powered security solutions such as Quick Heal AntiFraud.AI add an additional shield of protection against growing scams.