ET CISO.in
From The Economic Times

# Social engineering remains top reported attack vector in India

Social engineering attacks are increasingly prevalent in India, surpassing conventional threats such as malware and web applications. Various techniques, including phishing and shoulder surfing, are being employed by attackers to compromise sensitive data. Many incidents reported indicate that attackers exploit trust to manipulate individuals into sharing valuable information. Organizations are advised to implement multi-layered security systems and enhance employee training to mitigate such risks.

Social engineering remains the top attack vector reported by organisations in India, ahead of malware and web-application attacks, according to Seqrite's India Cyber Threat Report 2026. The report identifies several human-targeted attack methods, including shoulder surfing, phishing, vishing, smishing, impersonation and digital honey traps. It also highlights how attackers can exploit trust, attention, fear and routine behaviour to obtain sensitive information or gain access to systems.

Attackers can persuade employees to disclose information, scan malicious QR codes, approve login prompts, share one-time passwords (OTPs), install fake applications or open deceptive attachments.

Shoulder surfing and social engineering

Shoulder surfing remains a potential security risk 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 other confidential information on their devices. Information such as an employee ID, OTP, meeting subject line, tax document or visible screen notification can subsequently be combined with publicly available data and social engineering techniques to support fraud or intrusion attempts.

The report also identifies human-focused campaigns that do not initially rely on traditional malware. Digital honey traps can use AI-generated profiles, realistic photographs and crafted conversations on social media, dating platforms and messaging applications to establish trust before seeking workplace information, internal documents or private content.

## Shoulder surfing and social engineering

Shoulder surfing remains a potential security risk 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 other confidential information on their devices.
Information such as an employee ID, OTP, meeting subject line, tax document or visible screen notification can subsequently be combined with publicly available data and social engineering techniques to support fraud or intrusion attempts.
The report also identifies human-focused campaigns that do not initially rely on traditional malware. Digital honey traps can use Al-generated profiles, realistic photographs and crafted conversations on social media, dating platforms and messaging applications to establish trust before seeking workplace information, internal documents or private content.

## Security measures

The report recommends a layered security approach combining endpoint protection, identity monitoring, email and web controls, threat intelligence and behavioural analytics.
Behaviour-based security technologies, including next-generation antivirus and anti-ransomware engines, identified more than 34 million anomalous detections during the reporting period, according to the report.

Organisations are also advised to strengthen employee awareness through phishing and vishing simulations, role-based training, phishing-resistant multifactor authentication and behaviour-driven access policies.

Employees should independently verify unexpected requests and the identity of callers and senders, and report suspicious activity. Clear-screen practices, privacy filters, device-locking practices and caution when entering credentials in public spaces can also help reduce exposure to shoulder-surfing attacks.