CXO DIGITAL PULSE.COM
Tech@Rhythm of Business

Quick Heal Technologies Limited Reveals Key Insights into Rising KYC Scams in India

Pune, India: Quick Heal Technologies Limited today unveiled disturbing new insights into the rapid escalation of KYC-related fraud across India. As financial institutions, crypto exchanges and payment platforms continue to require digital identity verification, fraudsters have honed a variety of schemes-from phishing websites masquerading as official KYC portals to malicious Android apps disguised as legitimate verification tools-to harvest Aadhaar numbers, PAN details, selfies and one-time passwords. This stolen data fuels identity theft, unauthorized transactions and long-term financial damage for unsuspecting victims.

Quick Heal's investigation traces the KYC scam ecosystem from its phishing domains, often employing typosquatting and homoglyph tactics, to the back-end command-and-control infrastructure that exfiltrates data via HTTP POST requests or Telegram bots. Fraudulent SMS and email campaigns warn users of "incomplete KYC" or "account suspension," directing them to cloned sites that deceptively mimic bank branding and harvest credentials through simple HTML forms. In more advanced attacks, repackaged Android packages request excessive permissions, such as RECEIVE_SMS and SYSTEM_ALERT_WINDOW, to intercept OTPs, create fake overlays on banking apps and persist through device reboots.

Demographic analysis made by researchers at Seqrite Labs reveals that young professionals (ages 26-35) are the most frequently targeted group, accounting for roughly 25-30% of victims, followed by the 18-25 bracket at 18-22%. Middle-aged adults (36-50) form 20-25% of cases, while older adults and senior citizens comprise 12-15% and 5-8% respectively. Even minors fall prey, with 2-3% of victims under age 18. This broad age distribution underscores the sophistication of modern social-engineering tactics and the urgent need for public awareness.

With a sharp rise in the occurrence of digital fraud, Quick Heal Technologies Limited emphasizes the importance of a layered defense strategy. Behavioral-analysis solutions, such as Quick Heal AntiFraud.Al, flag anomalous app permissions, Al-based URL reputation scoring blocks look-alike KYC portals in real time, and SMS-and-call filtering prevents fraudulent "KYC update" prompts from ever reaching the user. Family members and caregivers are encouraged to discuss any unexpected verification requests with seniors or less tech-savvy individuals, reinforcing the human firewall. Furthermore, users should note that legitimate institutions will never ask for OTPs or official documents via WhatsApp, SMS or unsolicited email.