THE HINDU businessline.

Quick Heal warns of surge in 'digital arrest' scams

These scams typically begin with a phone call, email, or video message that appears to come from a legitimate authority figure

Quick Heal Technologies Limited, a global cybersecurity solutions provider, has detected a sharp rise in "digital arrest" scams across India. The company's latest analysis, prepared by researchers at Seqrite Labs—India's largest malware analysis platform—reveals that cybercriminals are increasingly combining leaked personal data with aggressive impersonation tactics to coerce individuals into transferring money or revealing sensitive information

According to Quick Heal, these scams typically begin with a phone call, email or video message that appears to come from a legitimate authority figure. Attackers fabricate allegations such as drug trafficking or money laundering and bolster their threats by citing accurate personal details. Much of this data have been harvested from large-scale breaches, including the April 2024 BoAt leak that exposed 7.5 million customer records and another breach involving Hathway documents containing Aadhaar and passport information.

By exploiting both fear and familiarity, scammers trick victims into visiting look-alike payment portals, entering card or UPI credentials, or installing remote-access tools that provide criminals full control over their devices.

Quick Heal's AntiFraud.AI platform has been developed to intercept such frauds. The cloud-assisted Fraud Call Alert flags spoofed numbers before the call is answered.

The company has urged users never to share one-time passwords, CVV codes or personal details during unsolicited communication. It also reminded the public that genuine government agencies do not demand payments via personal UPI handles, issue arrest warrants through email or conduct enforcement actions over platforms like WhatsApp or Zoom.