THE TIMES OF INDIA

How AI-generated deepfakes, phishing attacks may be a threat to 2024 elections

Seqrite report warns of AI threats and cybercrime disrupting elections, emphasizing ransomware defenses and collaborative efforts among CISOs to enhance cybersecurity posture against evolving risks in 2024. The India Cyber Threat Report adds that supply chain vulnerabilities also need collaborative cybersecurity efforts between the public as well as private sectors.

As India, and other countries prepare for elections, artificial Intelligence (AI)-generated deepfakes and other cybercrimes may disrupt the election process, a report has said, highlighting the need for collaborative efforts on this front. According to a report by Seqrite, the enterprise arm of global cybersecurity solutions provider Quick Heal, the upcoming 2024 elections are poised to attract phishing attacks exploiting political interests.

The India Cyber Threat Report adds that supply chain vulnerabilities also need collaborative cybersecurity efforts between the public and private sectors.

Cyber challenges in India in 2024

The report also anticipated emerging challenges that demand vigilance and strategic preparedness.

Apart from deepfakes, the report identified multi-factor authentication (MFA) fatigue attacks and complex ransomware incidents as the imminent threats for 2024 in India that require urgent attention

“With the rise of AI-powered threats like BlackMamba and the prevalence of Living off the Land attacks, Chief Information Security Officers (CISOs) must adopt advanced evasion techniques and heightened defences to combat evolving threats effectively,” the report said.

The report also stressed the need for strong defences against ransomware attacks. This includes practices like regular data backups, separating different parts of the network (segmentation), and quickly isolating any infected systems to prevent further spread.

“CISOs are encouraged to maintain vigilance regarding evolving cyber regulations and compliance standards, aligning security policies accordingly to ensure continual compliance and resilience,” the experts stated.

The report highlighted the significance of emerging technologies like AI, quantum computing, and IoT (Internet of Things), while remaining cognizant of the associated cybersecurity risks.

It underscored the importance of fostering collaborative relationships among CISOs and security professionals to collectively enhance organisations' cybersecurity posture and response capabilities.