ET CISO.in
From The Economic Times

Quick heal technologies: AI-powered cyber scams surge this diwali

Quick Heal warns of rising AI-powered cyber fraud during Diwali. Seqrite Labs reports criminals use AI for personalized attacks. Fake travel sites, e-commerce scams, and QR code traps target shoppers. Data breaches fuel sophisticated social engineering. Consumers must update devices, verify links, and report suspicious activity. Quick Heal offers AntiFraud.AI for protection.

E ETCISO Desk ETCISO Published On Oct 7, 2025 at 09:05 AM IST Read by 711

Quick Heal Technologies Limited, a global provider of cybersecurity solutions, today issued a comprehensive advisory warning consumers and businesses about an alarming escalation in sophisticated cyber fraud targeting the Diwali festivities. Researchers at Seqrite Labs, India’s largest malware analysis facility, reveal that cybercriminals are deploying artificial intelligence-powered tools to create highly personalized and contextual attacks.

Industry data indicates that e-commerce sales crossed ₹90,000 crore during Diwali 2024 alone, while Indian Railway Catering and Tourism Corporation (IRCTC) handled over 13 lakh bookings daily during peak season. This massive surge in digital transactions has created what researchers at Seqrite Labs describe as a "perfect storm" for cybercriminal exploitation. There has lately been a slew of impersonation messages specifically designed to target festival shoppers, many crafted to create artificial urgency and push users into clicking malicious links without proper verification.

Sneha Katkar, Head of Product Strategy at Quick Heal Technologies Limited, commented, “With GenAI coming into the picture, it becomes extremely easy for fraudsters to create communication that's customised and very contextual in nature. Festive inboxes often overflow with tempting 'lightning deals,' yet the most dazzling messages can be Trojan firecrackers. Fraudsters weaponise holiday FOMO, lacing subject lines with aggressive countdowns or threats of account suspension, signals that genuine merchants rarely deploy amid celebrations.”

Quick Heal Technologies Limited has identified five dominant attack patterns specifically targeting festival shoppers:

1.**Counterfeit Travel and Booking Portals**: Sophisticated fraudsters are creating convincing clones of IRCTC and major airline websites, often promoted through phishing emails, Google advertisements, and WhatsApp forwards. These fake booking interfaces collect personal details and payment information before siphoning money directly from victims' accounts. The company has documented cases where additional malware is injected into devices to steal future transactions.

2.**Malicious E-commerce and Shopping Scams**: Cybercriminals are establishing fake e-commerce websites advertising "lightning deals" and festival discounts that appear legitimate but serve as data harvesting operations. CloudSEK research referenced by Quick Heal identified 828 distinct domains devoted to phishing activities found in Facebook Ads Library, many specifically targeting festive season shoppers through typosquatting techniques that exploit common typing errors.

3.**Event and Entertainment Fraud**: The excitement surrounding pandal visits, dandiya nights, garba events, and other festive celebrations has created opportunities for criminals to exploit booking urgency. Quick Heal researchers have documented counterfeit ticketing sites and fraudulent UPI payment requests that redirect users to phishing pages designed to drain bank accounts instantly.

4.**QR Code and UPI Payment Traps**: QR-code scams have emerged as a widespread technique, often redirecting people to malicious sites that look deceptively real. These attacks have expanded beyond simple payment fraud to include complex redirection schemes that lead users to credential-harvesting websites disguised as legitimate festival shopping platforms.

5.**AI-Enhanced Social Engineering**: The integration of artificial intelligence has enabled cybercriminals to create highly personalized phishing campaigns that reference users' actual shopping patterns, search history, and social media activity. These sophisticated attacks are significantly more difficult to detect through traditional means.

Quick Heal Technologies Limited's analysis also reveals that cybercriminals are increasingly leveraging data from previous breaches to enhance their social engineering attacks. Significant data breaches exposing millions of customer records, including Aadhaar and passport information, provide criminals with authentic personal details that make impersonation attempts more convincing during festive fraud campaigns.

Researchers at Seqrite Labs have also identified concerning trends in "digital arrest" scams, where perpetrators initiate contact through phone calls, emails, or video messages appearing to originate from credible authorities. These sophisticated social engineering attacks fabricate accusations such as drug trafficking or money laundering while referencing accurate personal information obtained from previous data breaches.

Amidst this, Quick Heal Technologies Limited recommends that consumers update all devices, avoid clicking on unsolicited links, verify payment beneficiaries before authorising UPI transfers, and report suspicious activity immediately on cybercrime.gov.in. The company’s AntiFraud.AI, India's first AI-powered fraud prevention solution, delivers real-time phishing detection, scam-call alerts and dark-web monitoring to blunt these emerging threats.

The escalation of AI-powered cybercrime during India's festival seasons represents a critical inflection point for digital security. As festivals continue to drive increased online activity, Quick Heal Technologies Limited stresses that both technological solutions and behavioral awareness will be essential for protecting consumers and businesses from increasingly sophisticated threat actors.