ET CISO.in
From The Economic Times

Quick heal technologies urges users to stay vigilant as cybercriminals target festive celebrations

As India gears up for festive celebrations, Quick Heal Technologies warns of a surge in cyber scams targeting online travel bookings, event passes, and e-commerce deals. Fraudsters employ fake websites, phishing links, and malicious apps to steal personal and financial data. Experts advise vigilance, urging users to verify website URLs, update software, and use VPNs on public Wi-Fi.

As the festive season kicks off in India, Quick Heal Technologies Limited, a global provider of cybersecurity solutions, has raised the alarm about a predictable but nonetheless devastating rise in cyber scams. With festivals like Ganesh Chaturthi, Durga Puja, Diwali and Christmas fast approaching, an increasing number of people are heading to online travel portals such as IRCTC and leading airline websites to book train or flight tickets. Identifying this pattern, sophisticated fraudsters are laying traps in the form of convincing fake booking interfaces and bogus travel-package offers. Victims often discover too late that their personal and payment details have vanished into criminal hands.

The excitement of the season also draws people to book passes for pandals, dandiya nights and other festive events online. Criminals exploit that urgency by setting up counterfeit ticketing sites or sending UPI payment requests that lead to phishing pages. In the blink of an eye, shoppers who click a malicious link or approve a fraudulent UPI prompt find their accounts drained. Meanwhile, too-good-to-be-true e-commerce offers lure bargain hunters to cloned websites where hidden malware steals banking credentials, and festive greeting e-cards deliver mobile Trojans that exfiltrate contact lists and intercept OTPs.

Instant-credit and loan apps promising speedy approvals have become another battleground. Once installed, these fake applications demand excessive permissions - access to contacts, SMS messages and more then spread the scam by messaging victims' friends and family. Even well-meaning users who rely on public Wi-Fi at airports, railway stations or cafés may be caught in man-in-the-middle attacks that hijack their transactions or silently inject malicious code.

Behind nearly every successful attack lies a simple vulnerability: outdated software. During the holiday rush, it's common to postpone anti-virus updates and operating-system patches, leaving doors wide open for drive-by downloads and banking Trojans. Quick Heal Technologies Limited urges everyone, from festive planners to corporate holiday hosts, to treat online transactions with the same care they would a physical wallet.

"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. Impersonal greetings such as "Dear Customer" and hazy, off-brand graphics are additional red flags. When uncertainty lingers, bypass embedded links altogether by opening the brand's official app or typing its address yourself. Keep devices and banking apps updated, and lean on comprehensive fraud prevention tools such as Quick Heal AntiFraud.AI. Remember that intuition is a formidable shield: if an offer feels too spectacular to be real, it almost certainly is", said Sneha Katkar, Head of Product Strategy at Quick Heal Technologies Limited.

Consumers should always verify a website's URL and confirm the sender's details before entering any financial information. Only download apps like from official stores, enable automatic updates for all security and operating-system software, and use a virtual private network on public networks. One can also download Antifraud. Al which ensures the safety on the users. Also, regularly reviewing bank and UPI statements makes it possible to spot unauthorized transactions early, and sharing these safety practices with loved ones can prevent scammers from spreading through personal networks.