ET Edge INSIGHTS

India’s cyber fraud surge: Why festivals are prime time for hackers

As the first strains of festive music echo across India and markets light up with decorations, another kind of preparation is quietly underway—not in homes or temples, but in hidden corners of the internet. Cybercriminals are gearing up for their busiest season of the year, exploiting the collective euphoria of Ganesh Chaturthi, Durga Puja, Diwali, and Christmas to launch a barrage of digital scams.

Quick Heal Technologies Ltd, a global cybersecurity provider, has warned of a sharp spike in festive cyber fraud this year. The risks range from phishing portals disguised as ticketing websites to malicious greeting e-cards carrying hidden malware. And while the scams themselves vary, they share a single strategy: using the urgency, generosity, and excitement of India’s festivals as bait.

Festivals are synonymous with heavy spending in India—on travel, shopping, food, and gifts. According to industry reports, e-commerce sales alone crossed ₹90,000 crore during Diwali 2024, while IRCTC handled over 13 lakh bookings daily in peak season. For hackers, this flurry of digital transactions presents a perfect storm.

“The festive inbox overflows with offers and countdowns. Scammers know people are less cautious when they’re racing against time to grab deals or book last-minute tickets. That’s why festive seasons are prime time for cybercrime,” explains Sneha Katkar, Head of Product Strategy at Quick Heal Technologies.

This manipulation of urgency is deliberate. Fraudsters craft fake IRCTC portals, bogus airline booking sites, and even counterfeit dandiya or pandal passes. Victims, eager not to miss out, click before they think—only to find their bank accounts drained or credit cards compromised.

Travel scams take center stage

With lakhs of Indians traveling to be with family or visit hometowns, fake travel booking scams have become rampant. Fraudsters set up convincing clones of IRCTC or airline portals, often promoted through phishing emails, Google ads, or WhatsApp forwards.

Once users enter personal details and payment information, the money is siphoned off, and in many cases, additional malware is injected into their devices to steal future transactions.

Travel-related fraud is one of the most damaging because it not only causes financial loss but also ruins family plans. Imagine reaching the airport only to discover your ticket never existed.

Event tickets and UPI phishing

Beyond travel, hackers have expanded into festive eventsgarba nights, pandal entry passes, and Christmas concerts. Fraudsters set up fake ticketing portals or circulate QR codes and UPI links promising "early-bird discounts."

The scam plays out in seconds: once the UPI request is approved, the funds vanish. Victims often realize too late that no ticket confirmation will ever arrive.

In one recent case in Kolkata, cyber police reported dozens of Durga Puja enthusiasts duped through bogus pass-booking websites that mimicked legitimate organizers.

Shopping, loans, and "too-good-to-be-true" deals

The lure of festive discounts is another goldmine for scammers. Fake e-commerce sites and cloned brand pages sprout overnight, offering "70% off" on gadgets or gold coins. Clicking these links may lead not only to financial theft but also to silent malware downloads.

Fraudsters are also pushing instant-credit and loan apps. These apps demand access to contacts, SMS, and storage permissions that are later abused to blackmail users or spread scams to their networks.

The hidden threats: Wi-Fi, outdated systems, and e-cards

Not all scams are flashy. Some rely on subtle lapses in digital hygiene. Public Wi-Fi at airports, railway stations, and cafés is a common hunting ground for man-in-the-middle attacks. Criminals hijack browsing sessions, inject malicious code, or steal credentials without victims realizing.

Then there's the perennial issue of outdated software. In the rush of festivities, users often postpone antivirus updates and OS patches. These unpatched systems become easy prey for banking Trojans or drive-by downloads.

Even nostalgic gestures like sending festive e-cards are being weaponized. Cybercriminals attach Trojans within greeting files, which once opened, exfiltrate contacts and intercept OTPs.

Why smart people still fall for scams

One may wonder—why do scams succeed year after year despite constant warnings? Experts point to psychology.

1. **Urgency and scarcity bias**: Countdown timers, "last 2 tickets left," or "offer ends in 5 minutes" push users into impulsive decisions.
2. **Authority and familiarity**: Fake portals mimic trusted brands like IRCTC, Amazon, or Flipkart, lowering suspicion.
3. **Social proof**: Fraudsters circulate fake testimonials or reviews to lure victims.
4. **Emotional vulnerability**: Festivals are about family, generosity, and giving—values that scammers exploit to their advantage.

Katkar notes: “Intuition is a formidable shield. If an offer feels too spectacular to be real, it almost certainly is.”

Staying safe in the festive rush

Cybersecurity experts insist that a few proactive measures can drastically reduce risks:

- **Verify URLs and domains** before entering payment details. Fraudulent sites often have subtle spelling errors.
- **Avoid clicking embedded links** in emails or messages; instead, type the official website address directly.
- **Use only official app stores** to download shopping, banking, or travel apps.
- **Enable automatic updates** for operating systems, antivirus software, and banking apps.
- **Use a VPN** on public Wi-Fi networks at airports or stations.
- **Deploy tools like Quick Heal AntiFraud.AI** for proactive detection of phishing and fraud attempts.
- **Regularly review bank and UPI statements** to catch unauthorized transactions early.
- **Educate family members**, especially elderly or first-time digital users, about common red flags like “Dear Customer” emails or suspicious payment requests.

The role of businesses and regulators

While consumers must stay vigilant, responsibility doesn’t end with them. Airlines, e-commerce platforms, and ticketing services need stronger fraud detection systems and clearer communication channels. Financial institutions must continue refining real-time fraud alerts and transaction monitoring.

The government too has a role through awareness campaigns, faster cybercrime reporting mechanisms, and stricter action against fake app publishers and fraudulent domains. Initiatives like the National Cyber Crime Reporting Portal (cybercrime.gov.in) are steps in the right direction, but adoption and awareness remain patchy.

The bigger picture: A digital India under siege

India’s digital transformation has been unprecedented. in October 2024 UPI had 16.58 billion financial transactions in a single month, the opportunities for growth and for exploitation are immense. Festivals magnify both sides of this reality.

Cybercrime is no longer limited to urban elites. Rural users booking tickets online, students trying loan apps, or elderly parents opening e-cards are equally at risk. As digital inclusion grows, so must digital literacy.

Guarding the spirit of the season

Festivals in India are about togetherness, faith, and joy. But cybercriminals are adept at twisting these very sentiments into weapons. The cost of a single mistake can be more than money it can mean missed family reunions, lost trust, and lasting psychological scars.

This festive season, as the nation lights diyas and celebrates togetherness, it must also light up its digital defenses. Caution, awareness, and the right tools can ensure that the season remains one of joy, not regret.

The only rtule to follow is to treat your online accounts like your wallet. You wouldn’t hand it to a stranger in a crowded bazaardon’t hand your data to one in a digital marketplace either.