ET Edge
An Economic Times Initiative

Don’t let cybercriminals dim your Diwali light: 5 dominant cyber scam patterns to watch out for

Cyber Security / By Poonam Mondal

The festival of lights, Diwali, brings with it a wave of joy, celebration, and, of course, shopping. As Indians across the country gear up to buy gifts, electronics, clothes, and sweets, a darker trend also sees a significant spike: cyber scams. Scammers exploit the festive rush and the hunt for a good bargain, targeting unsuspecting shoppers with increasingly sophisticated tricks. This year, as you light up your homes, don’t let a cybercriminal dim your festive spirit.

Researchers at Seqrite Labs, reveal in the India Cyber Threat Report 2025 that cybercriminals are deploying artificial intelligence-powered tools to create highly personalized and contextual attacks.

5 dominant cyber scam patterns to watch out for this Diwali

Cybercriminals use the festive theme to make their scams appear legitimate and enticing. The escalation of AI-powered cybercrime during India’s festival seasons represents a critical inflection point for digital security. 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.

How to protect yourself and shop safely

A little bit of caution can go a long way in protecting you from financial loss and mental stress. Follow these simple steps for a secure shopping experience:

1. **If it's too good to be true, it probably is:** An iPhone for ₹5,000 or a designer saree for ₹500 is a major red flag. Be highly skeptical of deals that seem unbelievably good.
2. **Check the website URL:** Always look for the padlock symbol in the address bar and ensure the URL starts with https: . Double-check the spelling of the website name to ensure you are on the legitimate site.
3. **Never click on suspicious links:** Do not click on links received from unknown numbers or emails. If you want to check an offer from a known brand, type the official website address directly into your browser.
4. **Use secure payment methods:** Whenever possible, use a credit card for online payments, as they often offer better fraud protection than debit cards. Avoid making direct bank transfers to unknown sellers. Using the cash on delivery (COD) option on unfamiliar sites is also a safe bet.

5. **Understand UPI and QR codes:** You never need to enter your UPI PIN to receive money. Decline any request that asks for your PIN to get a payment. Similarly, be wary of scanning QR codes sent by strangers.
6. **Beware of urgency:** Scammers often create a false sense of urgency with messages like "Offer valid for 10 minutes only!" to pressure you into making a quick decision without thinking. Take your time to verify the offer.

What to do if you've been scammed

If you suspect you have fallen victim to a cyber scam, act immediately:

- **Contact your bank:** Inform your bank or card issuer to block your card and dispute the transaction.
- **Report the crime:** File an official complaint on the National Cyber Crime Reporting Portal at cybercrime.gov.in or call the national helpline number 1930. The sooner you report, the better the chances of recovering your money.
- **Change your passwords:** If you believe your login credentials for any account have been compromised, change the passwords immediately.

Enjoy the festival of lights with your loved ones, but stay vigilant online. A smart shopper is a safe shopper and Quick Heal Technologies Limited stressed that both technological solutions and behavioral awareness will be essential for protecting consumers and businesses from increasingly sophisticated threat actors Happy Diwali!