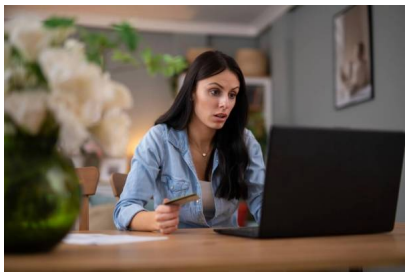
SUMMER TRAVEL SCAM SKYROCKET: FAKE WEBSITES MIMIC TRAVEL GIANTS



Summer travel peaks bring a surge in cyberattacks aimed at tourists. With holidays in full swing, hackers run organized operations mimicking well-known travel companies. Fake websites have multiplied quickly, according to analysts watching online threats. These pages copy real booking platforms almost exactly. Instead of reservations, they collect usernames, passwords, payment data. Behind the scenes, malicious networks harvest what users unknowingly submit.

Each fake portal acts like a digital trap disguised as convenience. Real logos, layouts, even customer support - faked perfectly. Visitors often realize too late that their details are already gone. Cybersecurity teams now warn travelers to double-check URLs before entering any private data to avoid the travel scam.

Come May, close to five hundred fresh sites tied to tourism firms got marked as harmful or questionable. That same month saw the creation of 47,318 new domain names connected to travel - up by a third compared to April and almost one-fifth more than last year at this time. Though plenty sit inactive, waiting quietly for high-demand seasons, every 112th one is now tagged as a threat.

Industrialized Digital Fraud

Operating like organized businesses, cybercriminals time their efforts to match market urgency and peak transaction periods. Instead of chaotic strikes, these groups launch timed initiatives - snatching domains that mirror current trends while rolling out region-specific travel scam pages designed to blend in. Their focus shifts with the calendar, aligning tricks to moments when people act fast and question little.

Among copycat sites, those mimicking Booking.com are especially noticeable. A fraudulent platform identified as bookingni[.]com aims to collect user credentials and credit details. Instead of genuine offers, versions like booking-cn[.]com and booking-hk[.]com display deals in Chinese currency alongside counterfeit discounts. Behind these is the same group running booking-jp[.]com and booking-zh[.]com.

Airbnb faces similar tactics. This fake site, airbnb-ca[.]com, zeroes in on travelers to Canada, showing pictures of mountain ranges alongside made-up rental options supposedly located in Montreal, Toronto, or Vancouver.

Hidden behind names like skyscanners[.]shop and skyscanners[.]life, counterfeit Skyscanner sites lure travelers with fake offers - especially early-bird prices on stays in Malaysia - that vanish after users pay upfront fees. These look-alike platforms take money without securing actual reservations.

Exploiting Urgency and Emotions

Summer travel plans often rush people into quick decisions. Scammers take advantage by pushing false deadlines like "prices go up soon" to spark fear. Unusually cheap offers appear too good to ignore, weakening careful thinking. Emotions run high when time feels short. These tricks work well because stress clouds judgment. Urgency replaces reflection. People act fast without checking

details.

A sharp rise stands out - incidents targeting travel services jumped 122% in three years. As travelers hunt discounts, scammers exploit moments of lowered attention. Data flows heavily through booking channels, creating tempting opportunities. Systems managing payments and identities become prime targets during these windows.

Additional Threats: WhatsApp Phishing

Messages arriving through chat platforms now carry risks just like counterfeit sites do. Lately, many people received notes pretending to be from Booking.com or actual hotels - targeting those who booked stays long ago. These messages usually ask for more money or fresh credit information, directing victims away from protected systems. Fraudsters rely on urgency, pushing replies before doubts arise.

Back then, similar signs appeared when Booking.com spotted odd behavior during a 2016 event, alerting customers that outsiders might have seen reservation data - names, home locations, emails, telephone numbers, plus whatever else guests shared with lodging providers. Though credit card records stayed safe, officials stressed this point clearly while urging awareness of possible travel scams targeting affected individuals afterward.

Expert Recommendations for Safe Booking

Security professionals urge travelers to adopt these protective habits:

- **Type, don’t click:** Manually enter the official URL into your browser instead of following links from emails, ads, or messages.
- **Verify the domain:** Carefully inspect the web address. A single extra letter or different extension can signal a fake website.
- **Use credit cards:** They generally provide stronger fraud protection and easier dispute processes than debit cards.
- **Enable 2FA:** Activate two-factor authentication on all travel accounts for an extra layer of security.
- **Beware of “miracles”:** If a deal seems too good to be true or creates excessive urgency, it likely is a travel scam.

It's worth noting - **trusted sites such as Booking.com avoid asking for payments through messages, calls, emails, or texts.** Instead, they handle transactions securely within their own system.

Summer travel brings busy times, so paying attention matters. When people remain aware - while using simple online safety steps - they guard both savings and private details during getaways. Enjoyment continues without compromise, given mindful habits along the way.

Date: 2026-06-22

Article link:
https://www.tourism-review.com/caution-travel-scam-and-fake-websites-multiply-news15518