BforeAI

May 2025

Threat Report: Phishing Tactics Targeting the Travel and Hospitality Sector

Airlines, Hotel and Lodging, and OTA Industries

TLP: WHITE

Executive Summary

The travel and hospitality industry is dynamic, growing, and incredibly lucrative, full of both classic traditions and new trends. According to the World Travel and Tourism Council (WTTC), the travel and tourism industry will contribute $11.7 trillion to the global economy, accounting for 10.3% of global GDP (gross domestic product). Against this impressive backdrop, it is important to highlight that the travel industry's success is also a magnet for cybercriminal activity.

With this in mind, the BforeAI threat research team at PreCrime Labs, sought to determine the level of travel-related scam activity being actively planned for the 2025 travel season. As a result, approximately 7500 domains were collected in the first 3 months of 2025, in which we identified scams targeting at least 86 distinct brands across the travel and hospitality industry.

Numbers and Statistics

PreCrime Labs identified over 5,000 newly registered travel-related domains and significant update activity to over 6,000 existing relevant domains in the first quarter of 2025. Considering the distribution of these domains, airlines accounted for less than 20% of the total number of domains collected, while the majority was taken by hotels and lodging categories (approximately 82%).

The largest portion of these domains (28%) were registered through GoDaddy (1418), followed by Namecheap, Inc. (448), PublicDomainRegistry (242), and Hostinger (209). Geographically, the United States accounted for the largest number of registered domains (1301), followed by Iceland (230), India (214), and China (195), highlighting the global nature of potential threats.

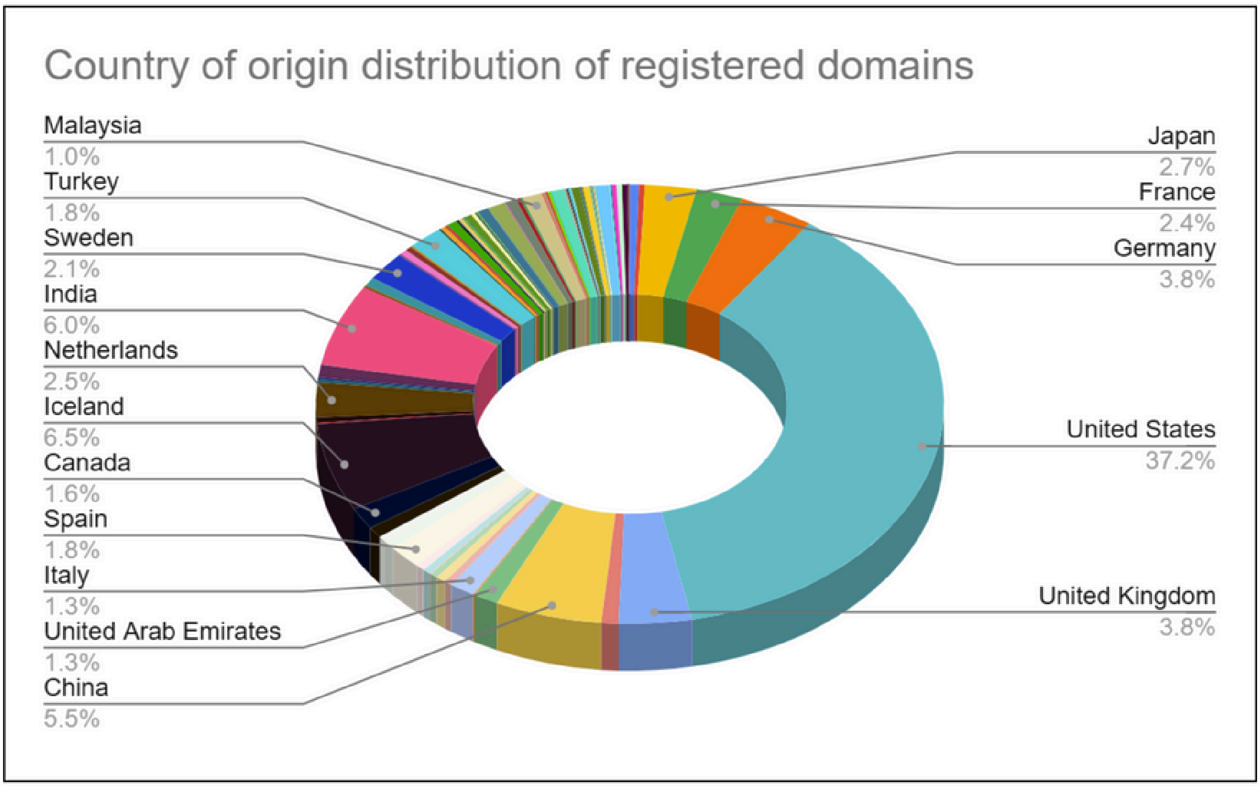


Figure 1: Distribution of domains according to their country of origin.

This period also saw a significant cluster of registrations generated through automated domain generation algorithms produced using artificial intelligence (AI). Such methods were deployed to create and register suspicious sites, by incorporating "AI" in their names, likely to offer AI-powered chatbots or similar services to facilitate travel customers.

For example, 17 domains sharing a similar domain pattern (e.g., web-booking-tiket-pesawat12344.de) were registered on the same day with changing numerical variables, raising concerns about coordinated malicious activity.

In addition to well-crafted impersonation sites mimicking genuine websites, several novel techniques were observed around airline loyalty programs and betting scams.

Recycling commonly-used scam themes, threat actors presented lures offering customized experiences, like local excursions or religious and cultural events, to drive more interest and engagement. The hotel and booking category hosted crypto scams, as well as fake third party services targeting vacation rental owners. In this category, PreCrime Labs determined that over 95% of new domains were suspected to be malicious.

Moreover, the scams expanded to include "special membership" programs requiring private group sign-ups for customized offers, the rise of fraudulent “travel buddy” job opportunities, fake recruitment schemes, and deceptive business coaching services.

Significant events across the globe greatly influence tourism trends, two such examples that stood out were the Maha Kumbh Mela pilgrimage in India, linked to 66 Indian hotel booking domains (discussed in more detail in the extended threat report) and similar, early indications of domains related to the Haj pilgrimage.

Based on Top Level Domain (TLD) distribution, it was clear that recognized and well-respected domains, with “.com”, “.org”, “.de”, “.net”, establish a trust factor among users, who are psychologically used to seeing familiar TLDs used by legitimate domains. However, to establish the sense of “limited offer” and “ending soon” deals, uncommon TLDs such as “.live”, “.shop”, “.store”, “.today”, “.vip”, “.world” were used. Some TLDs widely known to be associated with malicious activities were seen as well, such as “.xyz”, as a common example. The entire TLD distribution can be visualized here:

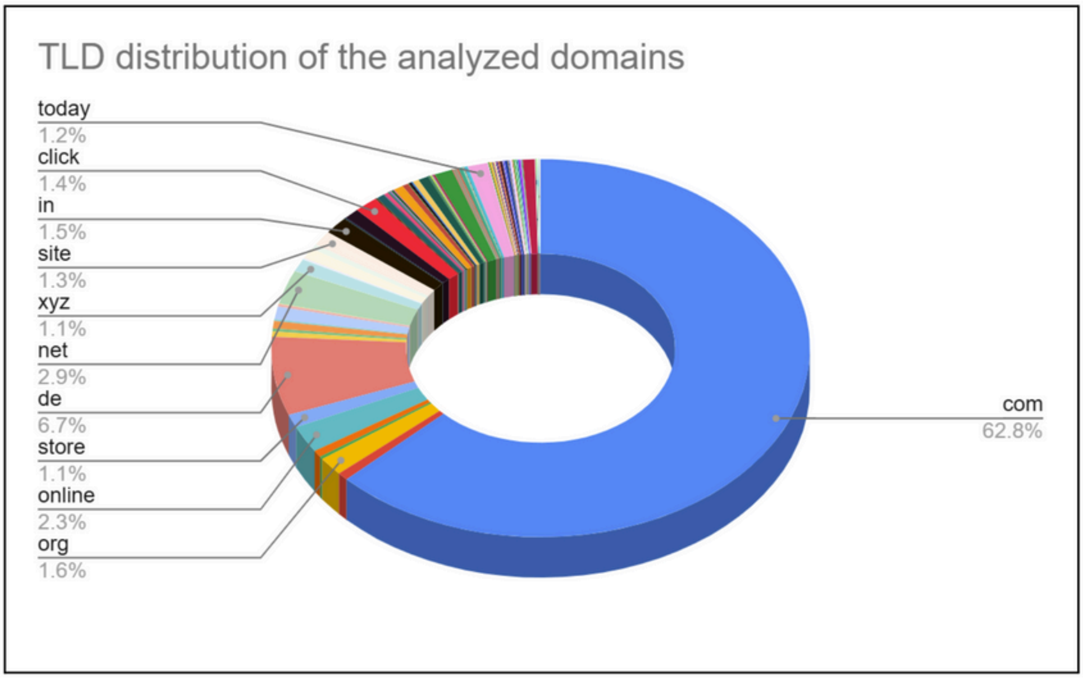


Figure 2: TLD distribution based on the malicious domain analysis.

Significant Campaigns

Offers and betting

A novel campaign was identified targeting users with a prediction game for airline fares, promising potential rewards (*Figure 3*). This activity was observed across both Indian, European, and U.S. carriers. Through phishing techniques such as typosquatting, threat actors replaced "fare" with "fair" followed by the name of the airline company, possibly to avoid detection. Notably, there was significant evidence of domain generation algorithms being utilized in this campaign.

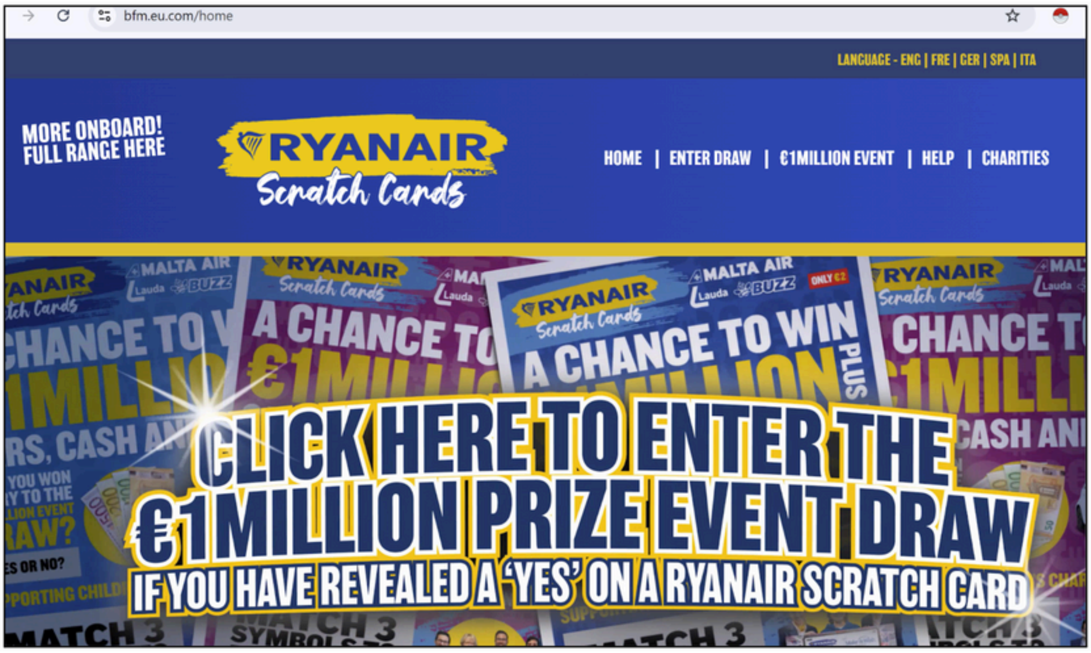
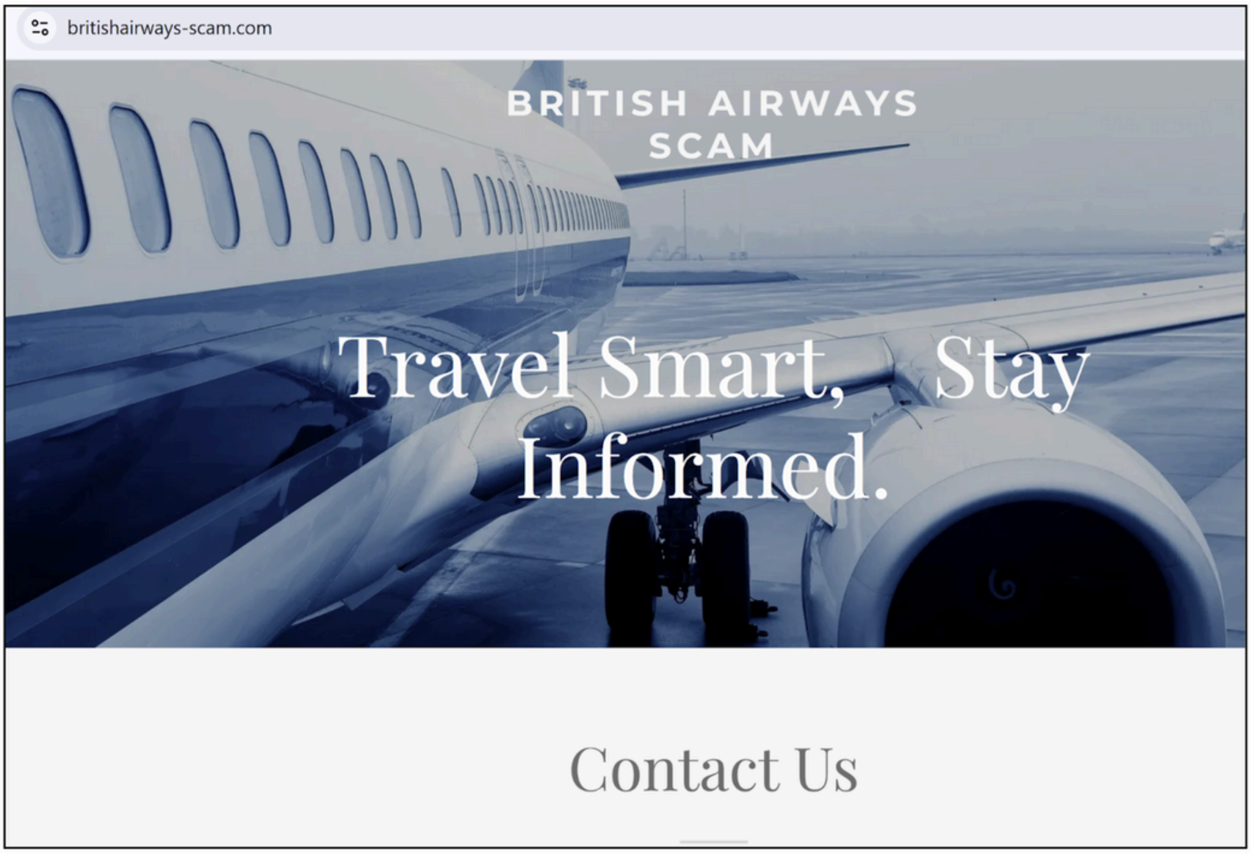

bfm.eu.com/home
LANGUAGE - ENG | FRE | GER | SPA | ITA
MORE ONBOARD! FULL RANGE HERE
RYANAIR Scratch Cards
HOME | ENTER DRAW | €1MILLION EVENT | HELP | CHARITIES
A CHANCE TO WIN €1MILLION PLUS
CLICK HERE TO ENTER THE €1MILLION PRIZE EVENT DRAW
IF YOU HAVE REVEALED A 'YES' ON A RYANAIR SCRATCH CARD

Figure 3: Example of a reward and betting site seen mimicking an airline offering the chance to win "deals" as a part of a phishing campaign.

Websites threatening to expose companies

Under the pretense of exposing perceived scams or to blame other airlines, hacktivist-led websites emerged purporting to reveal scams within the airline industry during the peak travel season. Keywords such as "exposed" and offensive languages were seen in this context, possibly to amplify negative sentiment. In addition to British Airways (*Figure 4*), fake websites were used in a similar context targeting West Jet that were yet to be developed and launched.



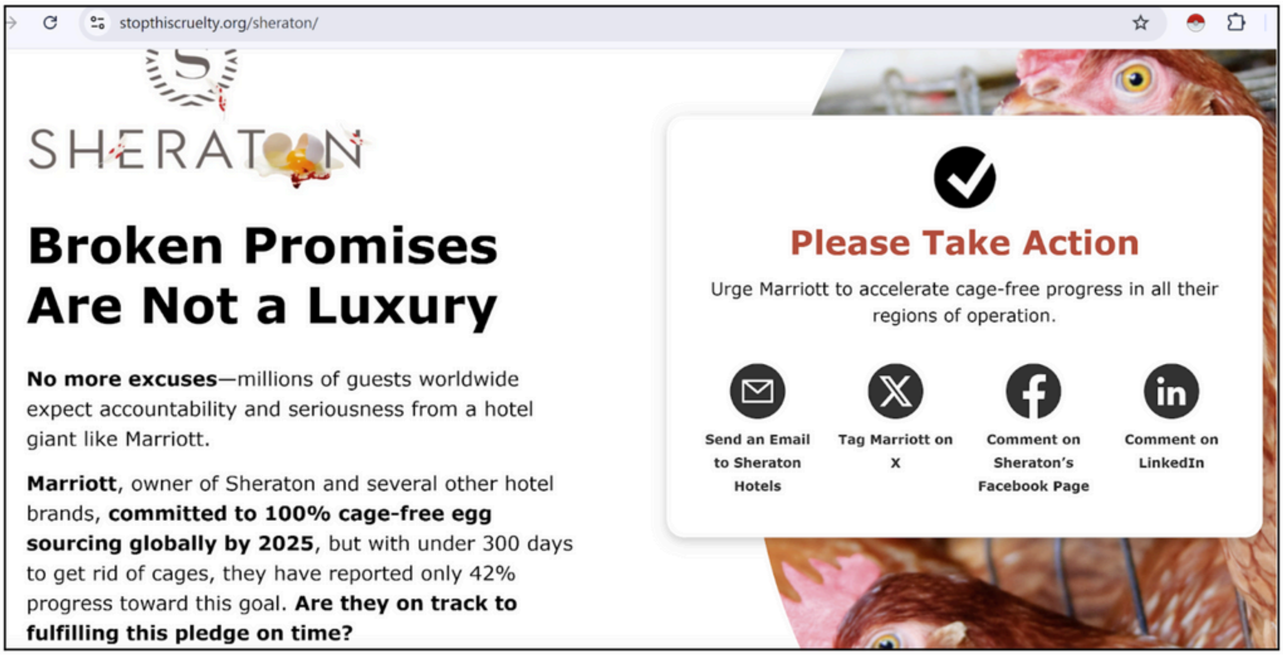
BRITISH AIRWAYS SCAM

Travel Smart, Stay Informed.

Contact Us

Figure 4: Trolling websites claiming to expose an alleged scam have the potential to negatively impact brand image.

Some websites, using generic domains, encourage widespread spamming by tagging hotel brands on social media, indirectly applying significant pressure and risking severe reputational damage. With the creation of multiple sub-pages, more hotel chains are vulnerable to these troll campaigns (*Figure 5*).



Broken Promises Are Not a Luxury

No more excuses—millions of guests worldwide expect accountability and seriousness from a hotel giant like Marriott.

Marriott, owner of Sheraton and several other hotel brands, **committed to 100% cage-free egg sourcing globally by 2025**, but with under 300 days to get rid of cages, they have reported only 42% progress toward this goal. **Are they on track to fulfilling this pledge on time?**

Please Take Action

Urge Marriott to accelerate cage-free progress in all their regions of operation.

Send an Email to Sheraton Hotels
Tag Marriott on X
Comment on Sheraton's Facebook Page
Comment on LinkedIn

Figure 5: Troll website targeting a hotel chain.

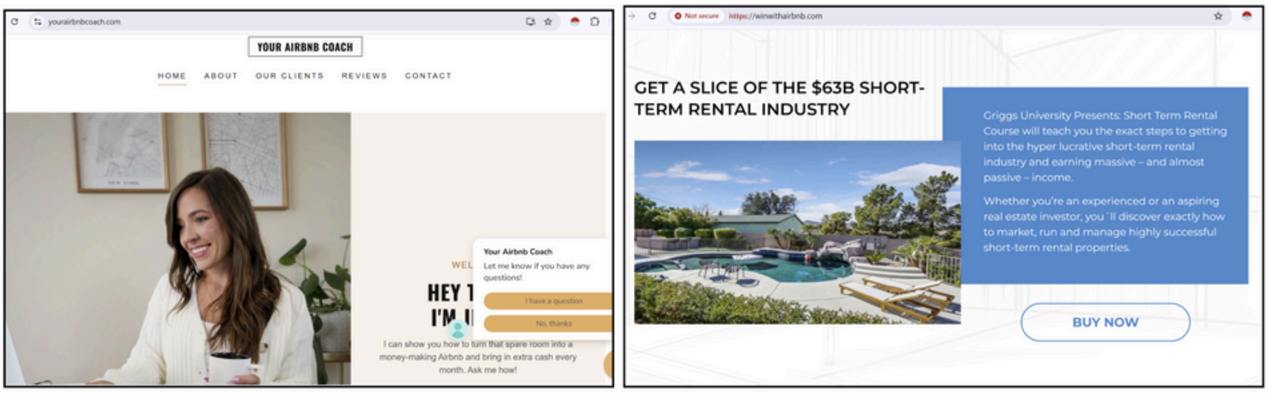
Cybercriminals may continue to focus on the efficiency offered by generic keyword methods to maximize umbrella phishing campaigns, making them operational as and when needed.

Mentorship and coaching to run a vacation lodging business

The premise of many vacation rentals or bed and breakfasts is for a property owner to use a private property to generate revenue by providing a localized lodging experience for travellers. The widespread popularity of these properties has given rise to individuals interested in profiting by subletting homes and apartments through platforms such as Airbnb. While many of these endeavors are successful, others are not, creating a vulnerable group of aspiring hosts targeted by newly-emerged “coaches” who provide guidance on “money-making” formulas to transform any property into a successful Airbnb listing.

Although some of these methods are legitimate, the claim that any space can be profitably converted is often false, leading to financial losses for those who invest in these unproven schemes and pay inexperienced "coaches" lacking relevant real estate expertise (Figure 6).

Interestingly, most such domains were seen associated with the keyword “Airbnb”.



Your Airbnb Coach
Let me know if you have any questions!

I can show you how to turn that spare room into a money-making Airbnb and bring in extra cash every month. Ask me how!

GET A SLICE OF THE $63B SHORT-TERM RENTAL INDUSTRY

Griggs University Presents: Short Term Rental Course will teach you the exact steps to getting into the hyper lucrative short-term rental industry and earning massive – and almost passive – income.

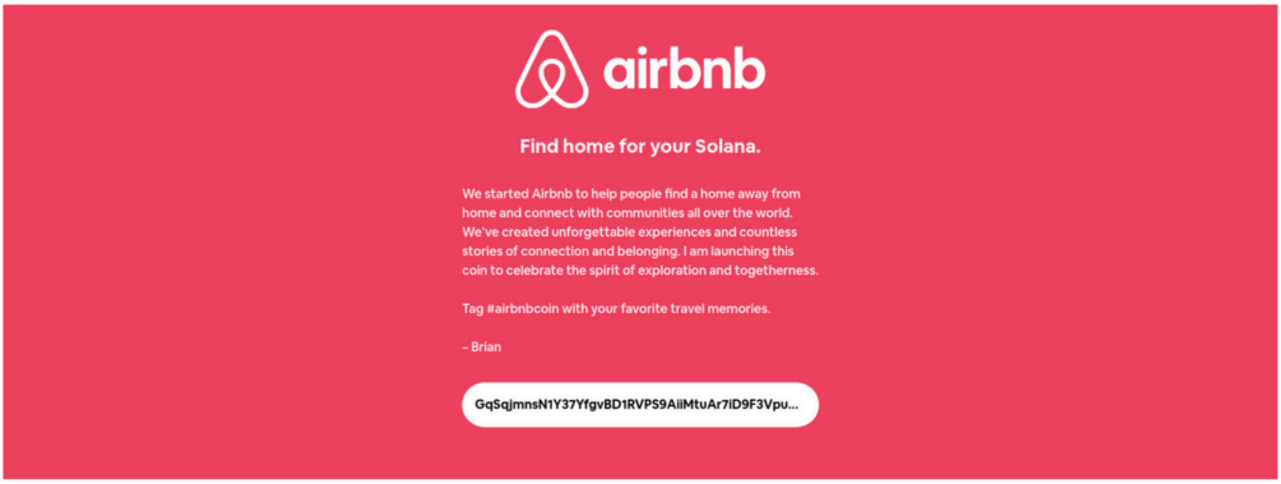
Whether you're an experienced or an aspiring real estate investor, you´ll discover exactly how to market, run and manage highly successful short-term rental properties.

Figure 6: Newly-emerged “coaches” shilling methods to successfully convert a space to Airbnb.

Additionally, the "coaching" and "mentoring" schemes for aspiring travelpreneurs or Airbnb hosts appear to be an emerging trend that will continue as long as the coaching theme stays relevant.

Hotels and lodging and their association with crypto coins

During the height of the travel season, cybercriminals falsely presented a website as a "celebration" of Airbnb, launching a coin with an address linked to an unverified part of the crypto world. The use of a genuine logo, coupled with minimal information beyond the address to track the coin, offers no way for unsuspecting users to verify the legitimacy of the launch, falling into a financial trap (*Figure 7*).



Find home for your Solana.

We started Airbnb to help people find a home away from home and connect with communities all over the world. We've created unforgettable experiences and countless stories of connection and belonging. I am launching this coin to celebrate the spirit of exploration and togetherness.

Tag #airbnbcoin with your favorite travel memories.

– Brian

GqSqjmnsN1Y37YfgvBD1RVPS9AiiMtuAr7iD9F3Vpu...

Figure 7: Crypto coin targeting well-known names in the hotel and lodging industry.

Additional findings

Malicious campaigns targeting the airlines industry

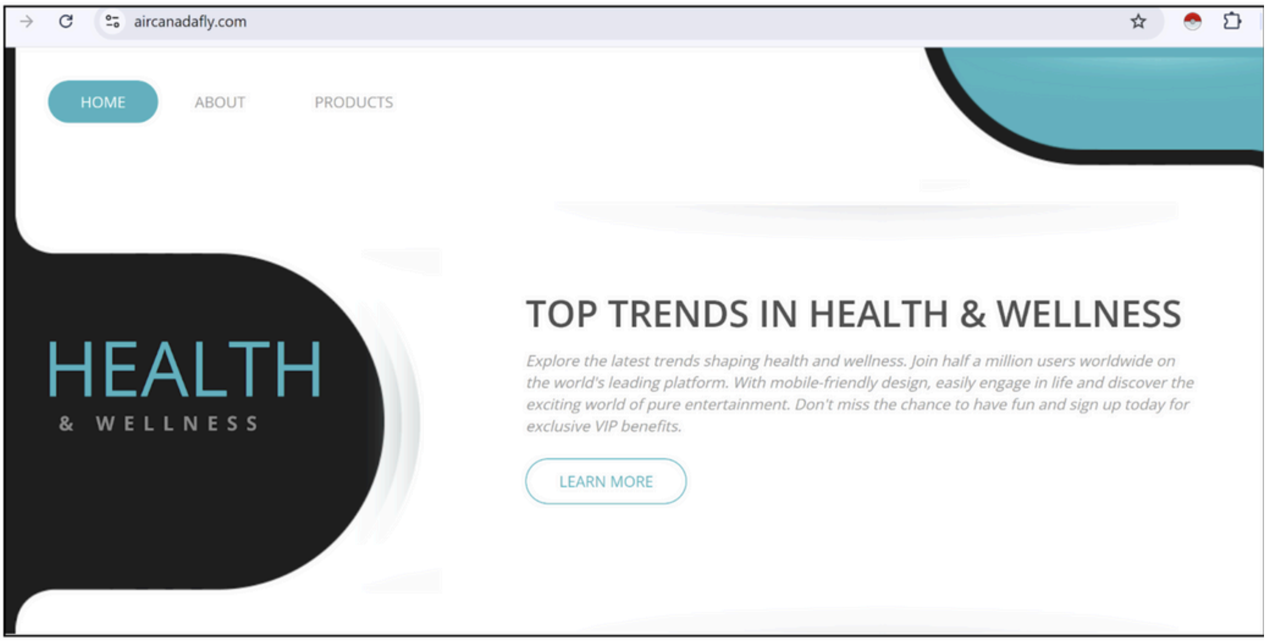
The airlines sector experienced a relatively low volume of suspicious domains compared with other sectors within the travel industry, with fewer than 1000 domains being identified. Globally prominent airlines such as Emirates, which faced the most targeting likely due to its diverse operations and businesses, followed by LATAM, and Indigo saw large volumes of phishing attempts. These along with 27 total airline brands were targeted to trick users into entering login credentials, payment info, or travel details — sometimes with minor typos (typosquatting) or added words like “express”, “shop”, or “booking” (keyword stuffing).

One of the biggest trends observed across the entire travel industry is the elevated use of AI as a service to enhance the customer experience (e.g., customer service bots, etc.). Many fraudulent websites attempted to leverage this AI trend to impersonate support/automated systems.

Common motivations behind phishing campaigns like the ones observed are credential theft, recruitment fraud, agency and travel platform scams, malware or fake downloads, and brand impersonation.

Post-campaign pivot

Although some observed phishing websites shifted their focus to other sectors on completion of but the executive summary ones have to be high level, business related, customer related, their previous campaign, their original airline-related domains subtly hint toward past activity targeting the travel industry. A considerable number of these sites now redirect elsewhere, possibly reflecting the decrease in travel demand after the peak season (Figure 8).



TOP TRENDS IN HEALTH & WELLNESS

Explore the latest trends shaping health and wellness. Join half a million users worldwide on the world's leading platform. With mobile-friendly design, easily engage in life and discover the exciting world of pure entertainment. Don't miss the chance to have fun and sign up today for exclusive VIP benefits.

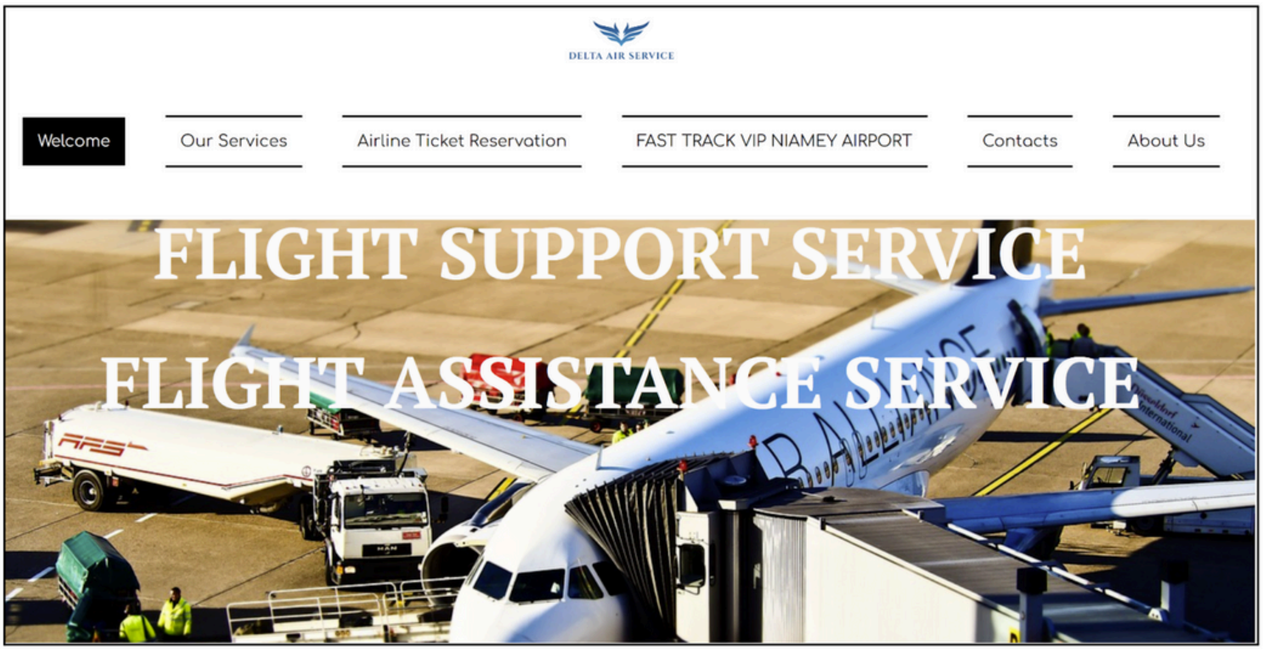
Figure 8: Phishing campaigns registered for airlines now pivots post campaign conclusion

In case of Air India, a campaign including a notable combination in a domain titled, “airindiapost” was seen, indicating a tricky combination of the airline name with the national post service. Such combinations can help cybercriminals rotate from one campaign to another without altering the core domain or to occasionally suggest interrelated services like sending parcels via the airline's postal network. This quarter saw instances of service mutation using common terms as a recurring technique.

Identical replica of the legitimate site

Airlines specializing in short haul domestic flights or offering “last minute” deals and booking options appeared to be more frequent targets, as they leverage a sense of urgency to reduce caution. Whereas travelers planning in advance were less likely to fall for these types of scams.

Brand impersonation was a common tactic used by criminals to fool customers into entering personal or financial information to execute fake bookings. Replicas of the legitimate airline websites, utilizing brand logo, look, and voice are common. In the case of personal information collection, this data can be used in future phishing and spearphishing campaigns (*Figure 9*). In cases where payments are made to purchase a ticket, the money is collected, but no ticket (or a fake ticket) is issued.



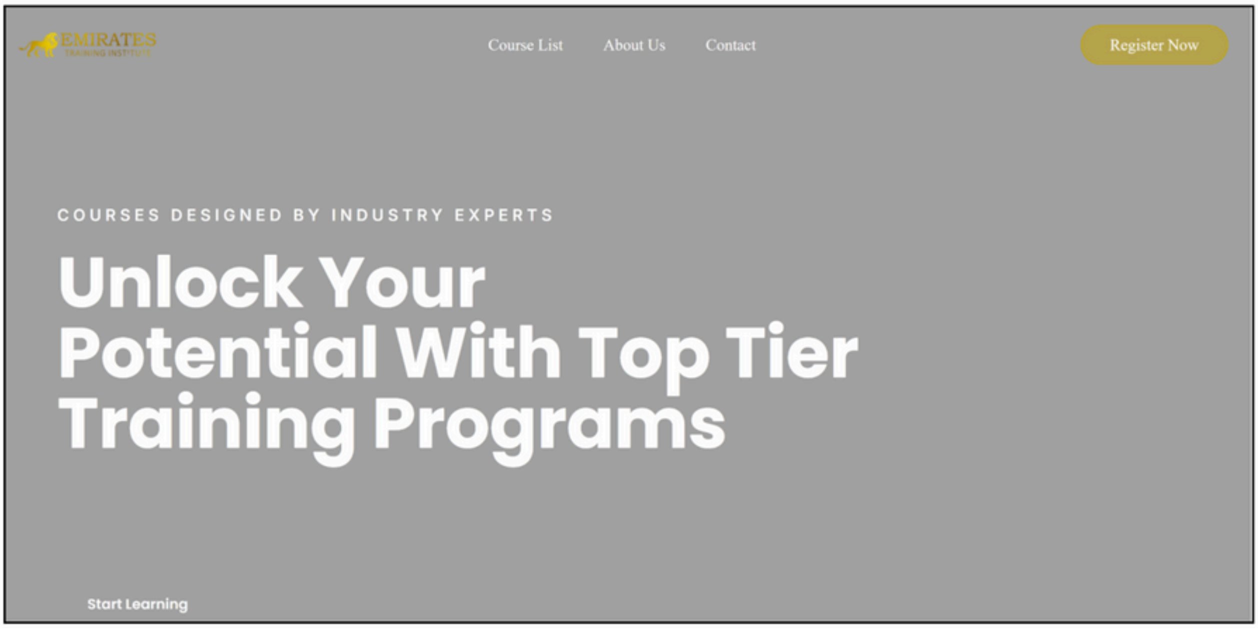
FLIGHT SUPPORT SERVICE

FLIGHT ASSISTANCE SERVICE

Figure 9: Replica of an original website seen as a part of a phishing campaign

Recruitment and trainings

Beyond targeting multiple customer-facing avenues of the airline industry, cybercriminals expanded their reach to employees, both current and aspiring candidates for hire. This was evident through different themes including job portals, cabin crew training programs (*Figure 10*). Instances featuring management login pages and airport office websites with login features were observed to target employees based on the airlines as well as specific airports.



COURSES DESIGNED BY INDUSTRY EXPERTS

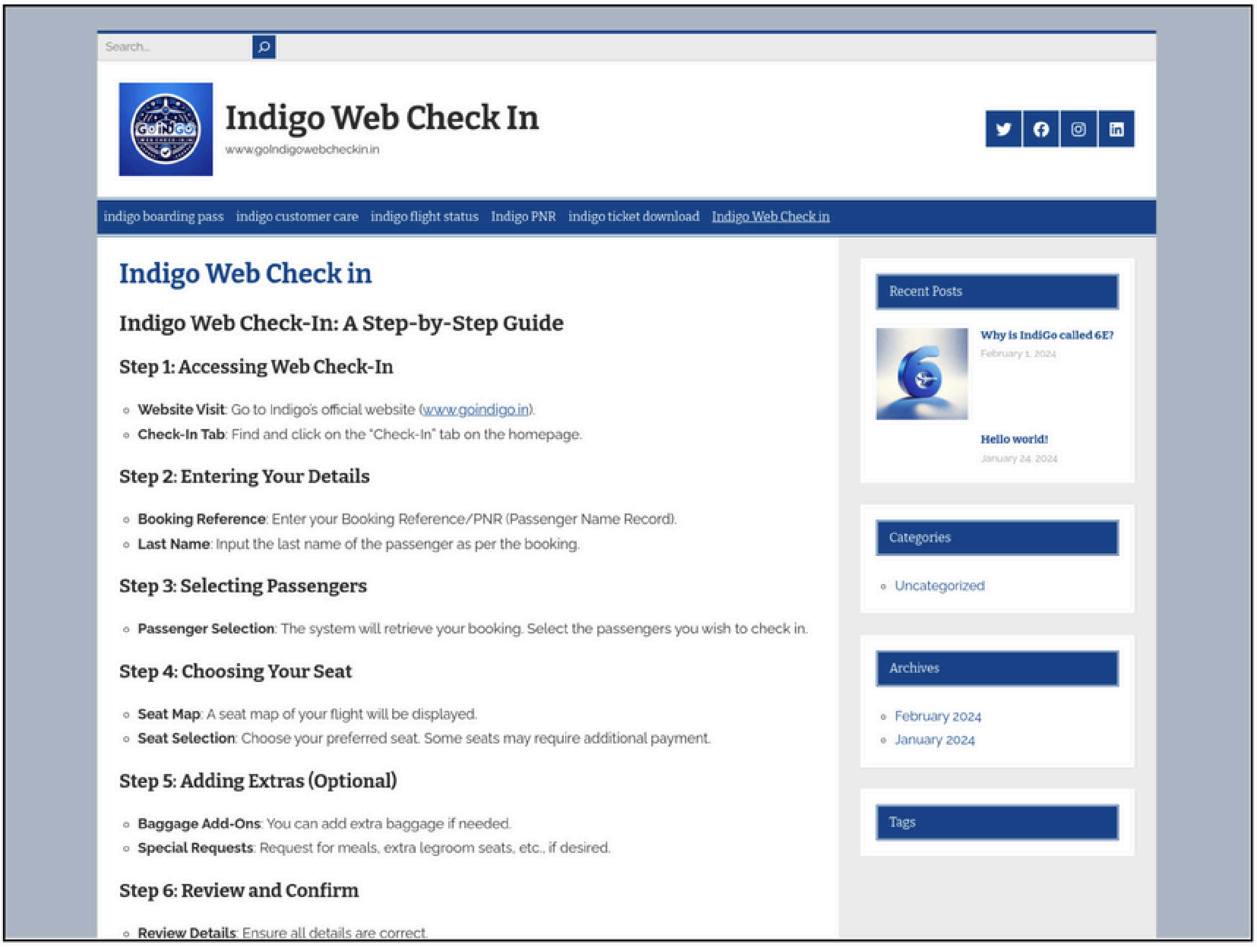
Unlock Your Potential With Top Tier Training Programs

Figure 10: Airlines added wing– cabin crew training targeting by cybercriminals to attack aspiring employees

Airline-related features and customization

Various features that are an integral part of the customer journey on an airline booking website were major targets, leaving no stone unturned. This included schemes for web check in, movers and packers, fraudulent airline-branded credit cards (*Figure 11*), management/employee login websites, local city office of the airline, and car rental services from airports.

Another prominent example was the creation of new suspicious booking aggregators for the travel industry. Such sites hosted multiple redirects to scammy URLs disguised as alternate package providers.



Indigo Web Check in

Indigo Web Check-In: A Step-by-Step Guide

Step 1: Accessing Web Check-In

- **Website Visit**: Go to Indigo's official website (www.goindigo.in).
- **Check-In Tab**: Find and click on the "Check-In" tab on the homepage.

Step 2: Entering Your Details

- **Booking Reference**: Enter your Booking Reference/PNR (Passenger Name Record).
- **Last Name**: Input the last name of the passenger as per the booking.

Step 3: Selecting Passengers

- **Passenger Selection**: The system will retrieve your booking. Select the passengers you wish to check in.

Step 4: Choosing Your Seat

- **Seat Map**: A seat map of your flight will be displayed.
- **Seat Selection**: Choose your preferred seat. Some seats may require additional payment.

Step 5: Adding Extras (Optional)

- **Baggage Add-Ons**: You can add extra baggage if needed.
- **Special Requests**: Request for meals, extra legroom seats, etc., if desired.

Step 6: Review and Confirm

- **Review Details**: Ensure all details are correct.

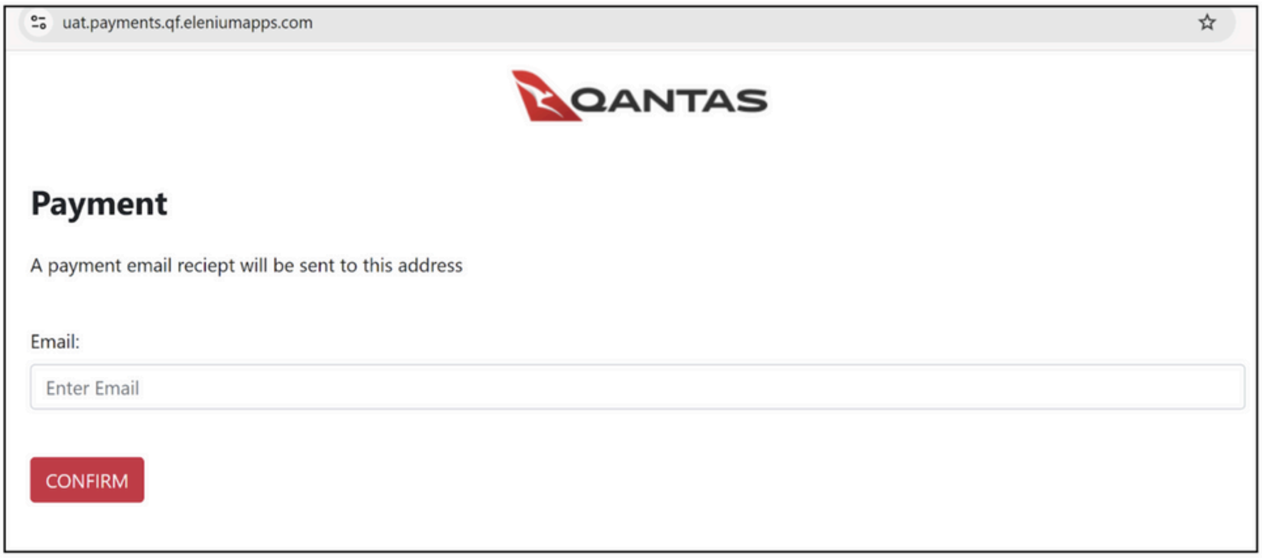
Figure 11: Web check-in guide apart from the official website should be treated with caution

Membership and loyalty programs

Airline loyalty and membership programs are frequent targets for scams. A variety of potential tactics are used with the end result being loss of money or loyalty points or the harvesting of personal data for future phishing campaigns.

A fake Qantas Airways frequent flyers login page (*Figure 12*) was found hosted under the domain name (oilandgasindustryjobs[.]com), indicating how threat actors disguise their scams using completely unrelated industry themes. We also observed use of free web app hosting to collect payments under the same offerings.

Airlines that have their own travel card were targeted in phishing attempts to harvest card related data. These malicious pages were often hosted on free services like Elenium Apps. Moreover, some scams offered cash back on flights to gather travel details, flying history, and even boarding details, all considered to be sensitive flyer data.



uat.payments.qf.eleniumapps.com

QANTAS

Payment

A payment email reciept will be sent to this address

Email:

Enter Email

Figure 12: Free hosting platforms targeting the airline industry through their frequent flyers program

Hotel and lodging scams

The hotel and lodging category comprised the majority of the dataset identified as malicious over the first quarter of 2025. A new range of threats were seen that diverged from the traditional methods of typosquatting or impersonating legitimate websites.

PreCrime Labs analysis uncovered a massive, persistent wave of malicious domain registrations exploiting the global hotel and lodging sector. From luxury resorts to vacation rental platforms like Airbnb, threat actors are creating fake digital infrastructure designed to impersonate brands, deceive travelers, and harvest credentials or financial data.

Domain trends seen in the recent suspicious registrations

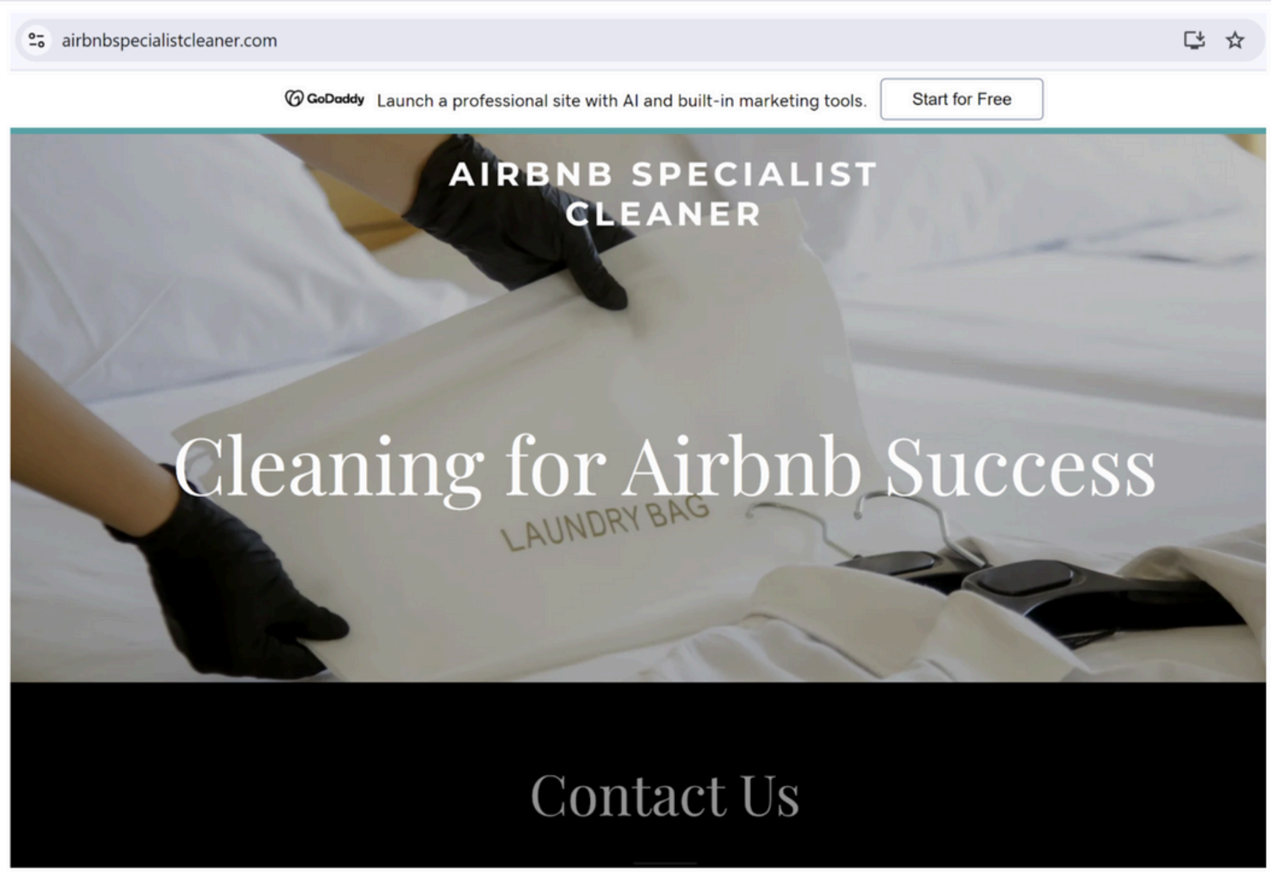
We observed the upcoming AI trend blending effortlessly in this industry through strategically positioned domains such as “Chatgpt Hotels”, and AI hotel booking features. Approximately 120 domains featuring keywords like “luxury-hotels”, “exclusive-adults-only-hotels”, “spa”, “wellness” were used to trick travelers seeking a premium lodging experience. There’s a notable presence of fake “concierge” or “management” services related to these domains.

A significant observation is the cluster of 430 domains using “Airbnb” as a keyword, incorporating terms such as “cleaner”, “reservation”, “booking”, “concierge”, “dispute”, “coach”, and “mentor”. Additionally, phishing attempts related to experiential add-ons included in a trip such as “things to do” and “places to see”, have evolved as per geographical distribution.

For instance, fake yacht booking sites were observed in coastal regions like Dubai and Mumbai. Similarly, safari-themed phishing domains emerged targeting areas with jungles and deserts, highlighting the growth of dedicated experiential sites as a distinct attack vector. Some of the prominent examples are seen as follows:

Third party services

Renting out a property typically requires either internal cleaning management or the engagement of external services for maintenance. That said, many third party services emerged to offer cleaning services. Unfortunately, many of these websites were poorly made, and might ask for prepayment, after which the services ordered may never materialize (*Figure 13*). It is essential to beware of recently formed companies with a basic template, and signs of poor professionalism to avoid being a victim.



airbnbspecialistcleaner.com

GoDaddy Launch a professional site with AI and built-in marketing tools.

AIRBNB SPECIALIST CLEANER

Cleaning for Airbnb Success

Contact Us

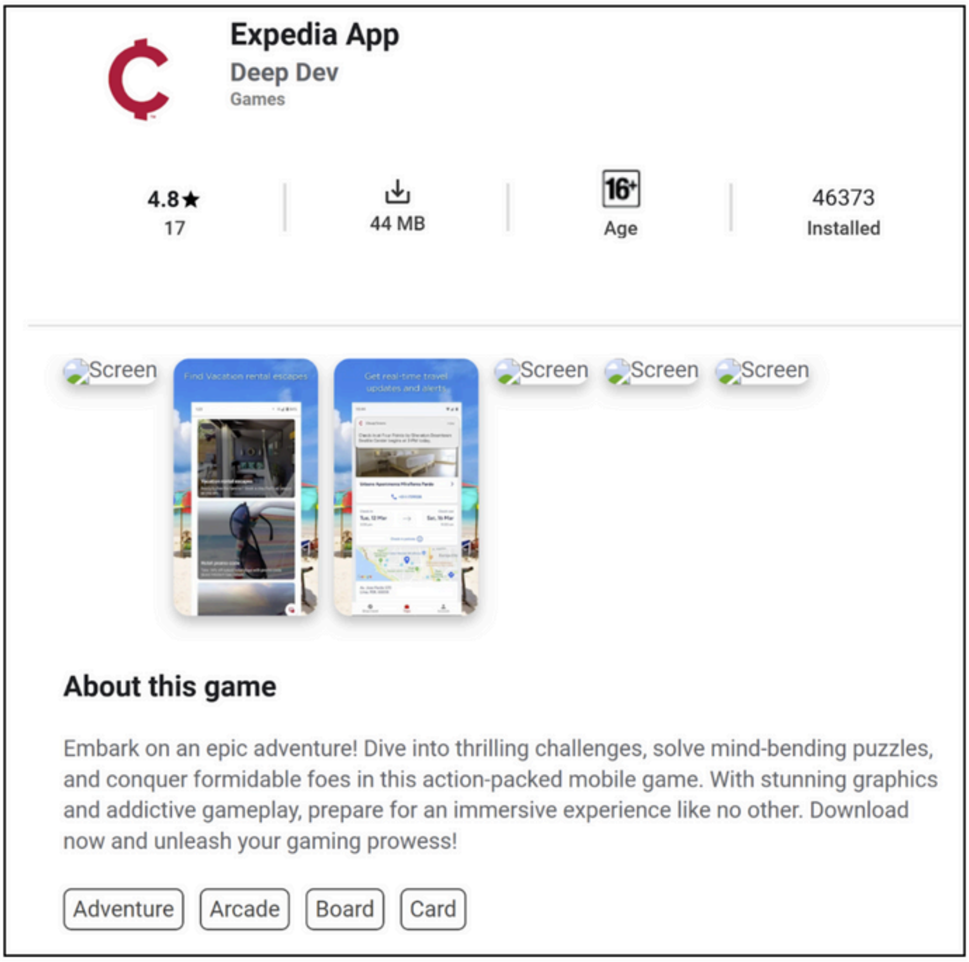
Figure 13: Newly emerged cleaning services with standard templates, making it suspicious

OTAs and travel aggregators targeted

Online travel agencies present one of the most common ways many consumers search for travel options and book trips for both personal and professional purposes. All-in-one platforms like Expedia, Kayak, Agoda and several others are often the targets of impersonation scams, among other cyber crimes. The definition of an OTA can be a bit murky, as many other travel vendors (like hotels and vacation rental sites) offer packages that include flights, car rentals, tours and experiences, and more. However, traditional OTAs and aggregators are prime targets for cybercrime, as they often sell packages of sizable value, and therefore offer a lucrative payout if a fraudulent booking is successful.

Fake applications

Most Android users download travel aggregation applications from verified sites, bypassing third party websites. However, cybercriminals attempted to replicate the entire template of the Google Play Store to offer Expedia apps (*Figure 14*). Some unusual elements such as categorizing the app as a "game" and broken structure are present, making it evident to a redirected user that they are not interacting with a legitimate site.



About this game

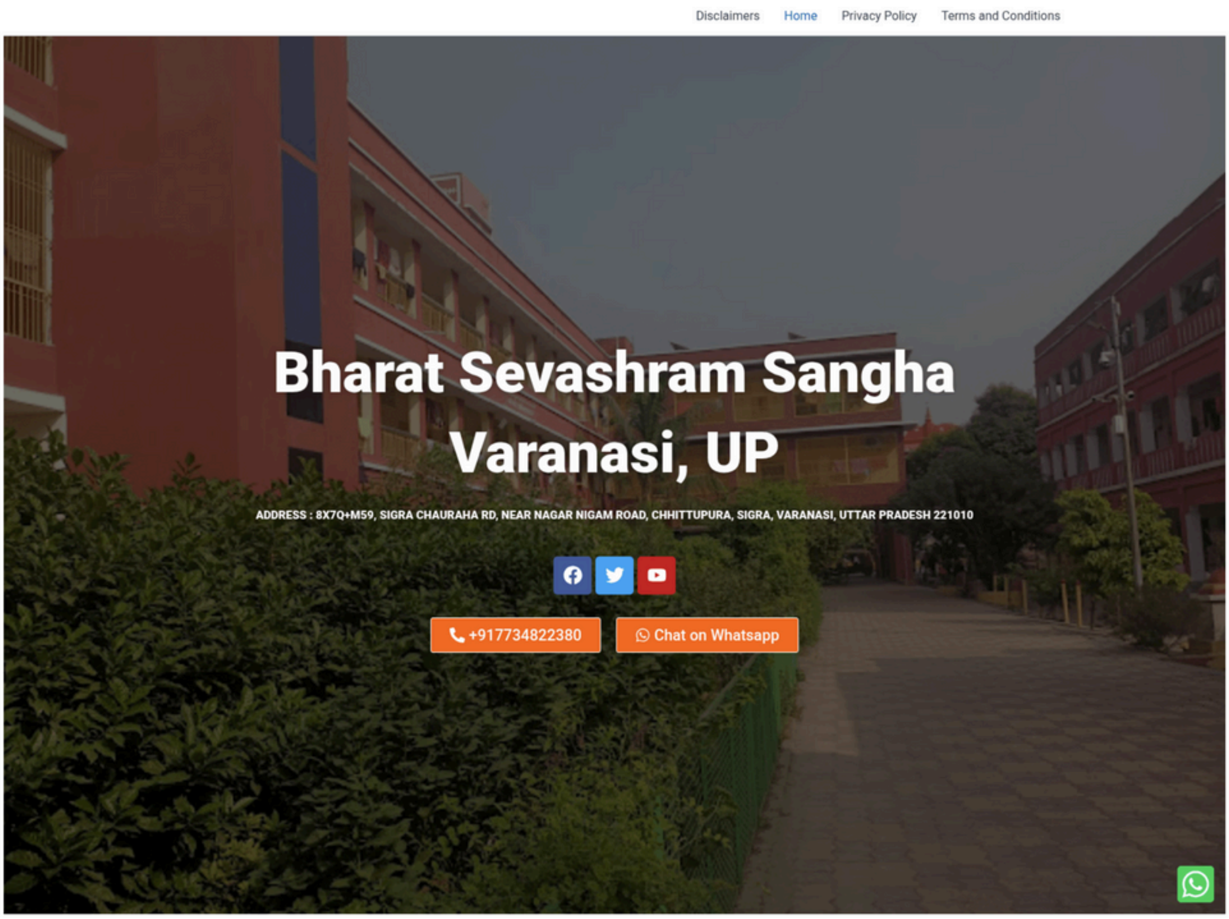
Embark on an epic adventure! Dive into thrilling challenges, solve mind-bending puzzles, and conquer formidable foes in this action-packed mobile game. With stunning graphics and addictive gameplay, prepare for an immersive experience like no other. Download now and unleash your gaming prowess!

Figure 14: Expedia App category offered as a game on a phishing site.

Significant religious events during and post travel season

Significant events drive travel any time of the year, and this year's Mahakumbhmela in India drew a large number of pilgrims seeking transportation to nearby locations (*Figure 15*). This led to Indian booking sites rapidly emerging without any verification of it being a legitimate business. Due to the limited duration of these religious gatherings, these websites come and have even been diverted to another irrelevant instance quickly.

Mirroring the phishing trend of religious pilgrimage, the upcoming Hajj pilgrimage to Mecca in Saudi Arabia is already showing subtle signs of bookings and domain registrations. This targets either accommodations in Saudi Arabia or different airlines serving the region. This pattern suggests that domain registrations related to major travel events often begin several months in advance of the actual occurrence.



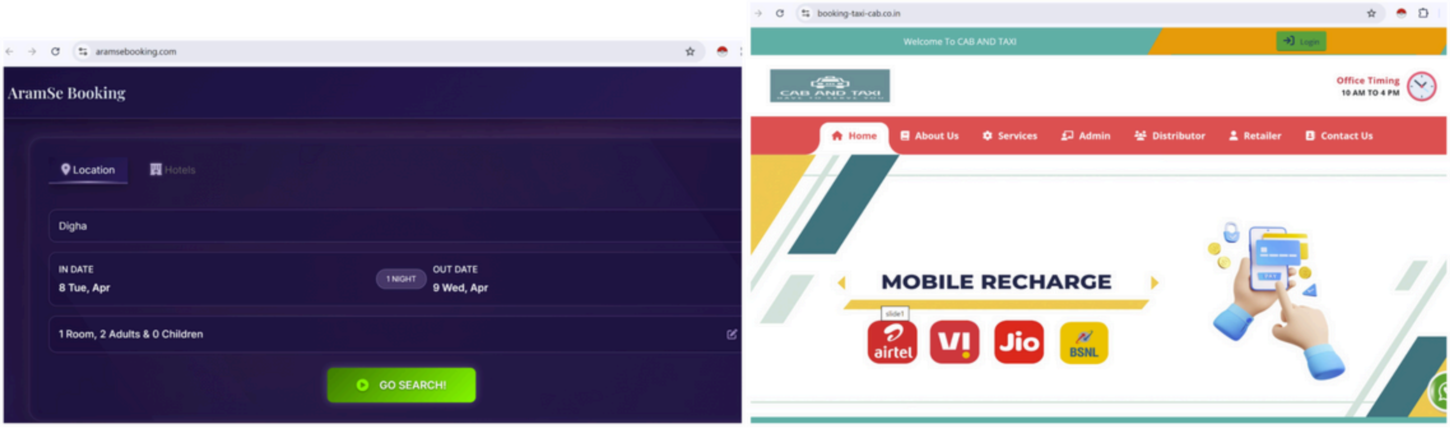
Bharat Sevashram Sangha Varanasi, UP

ADDRESS : 8X7Q+M59, SIGRA CHAURAHA RD, NEAR NAGAR NIGAM ROAD, CHHITTUPURA, SIGRA, VARANASI, UTTAR PRADESH 221010

Figure 15: An unverified website offering stay and services to the pilgrims during their visit to Mahakumbhmela in India

Rise of different booking platforms

Various websites and booking platforms emerged with diverse schemes to attract users. However, there are various red flags that could alert the users to potential scams, including recently created websites. Other attributes include a lack of integrated features like real-time tracking or payment processing, and irrelevant contextual information. Provided below (*Figures 16 & 17*) are two such examples, where a taxi booking website was also offering mobile recharge services across different telecom companies, raising suspicion.



Digha

8 Tue, Apr

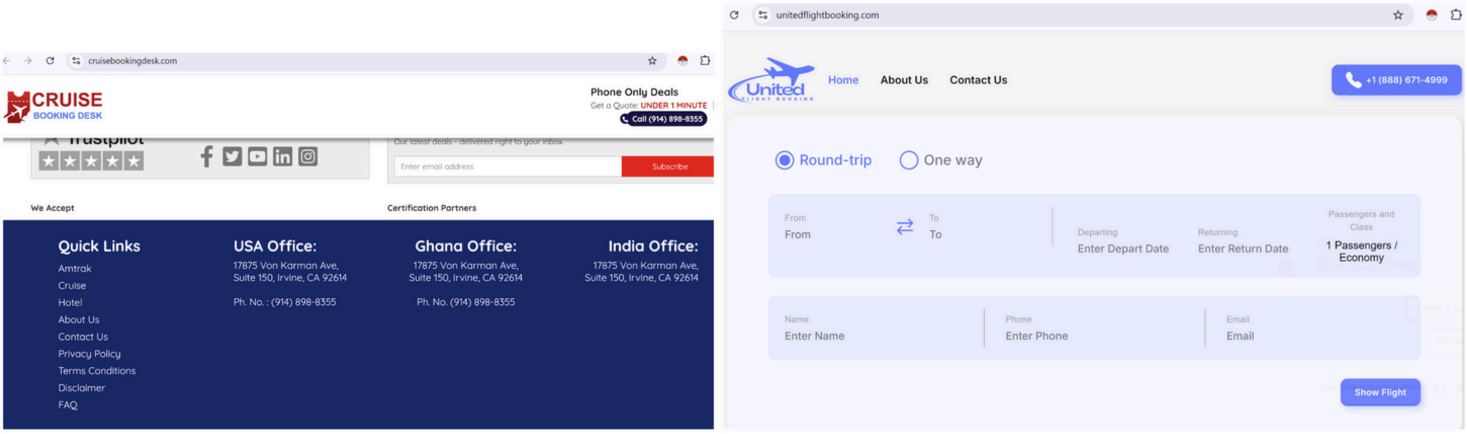
9 Wed, Apr

1 Room, 2 Adults & 0 Children

Figures 16 & 17: Threat actors registering new websites to bring up new booking agencies during travel season.

In another instance, the PreCrime Labs team identified multiple websites exhibiting basic template errors, and the formation of new booking companies using names closely resembling established brands. For example, the company “United Flight Booking” is thematically similar to United Airlines, and the cruise company mentioned in the below example (*Figures 18 & 19*) has the same address across all the branches in the USA, Ghana, and India.

These significant errors undoubtedly raise suspicions about the true existence of these companies and whether they genuinely offer reliable services to travelers.



cruisebookingdesk.com

CRUISE BOOKING DESK

Phone Only Deals
Get a Quote: UNDER 1 MINUTE
Call (914) 898-8355

Trustpilot

Our latest deals - delivered right to your inbox.

Enter email address | Subscribe

We Accept

Certification Partners

Quick Links
Amtrak
Cruise
Hotel
About Us
Contact Us
Privacy Policy
Terms Conditions
Disclaimer
FAQ

USA Office:
17875 Von Karman Ave,
Suite 150, Irvine, CA 92614
Ph. No. : (914) 898-8355

Ghana Office:
17875 Von Karman Ave,
Suite 150, Irvine, CA 92614
Ph. No. (914) 898-8355

India Office:
17875 Von Karman Ave,
Suite 150, Irvine, CA 92614

unitedflightbooking.com

United FLIGHT BOOKING

Home | About Us | Contact Us | +1 (888) 671-4999

● Round-trip ○ One way

From: From ⇄ To: To | Departing: Enter Depart Date | Returning: Enter Return Date | Passengers and Class: 1 Passengers / Economy

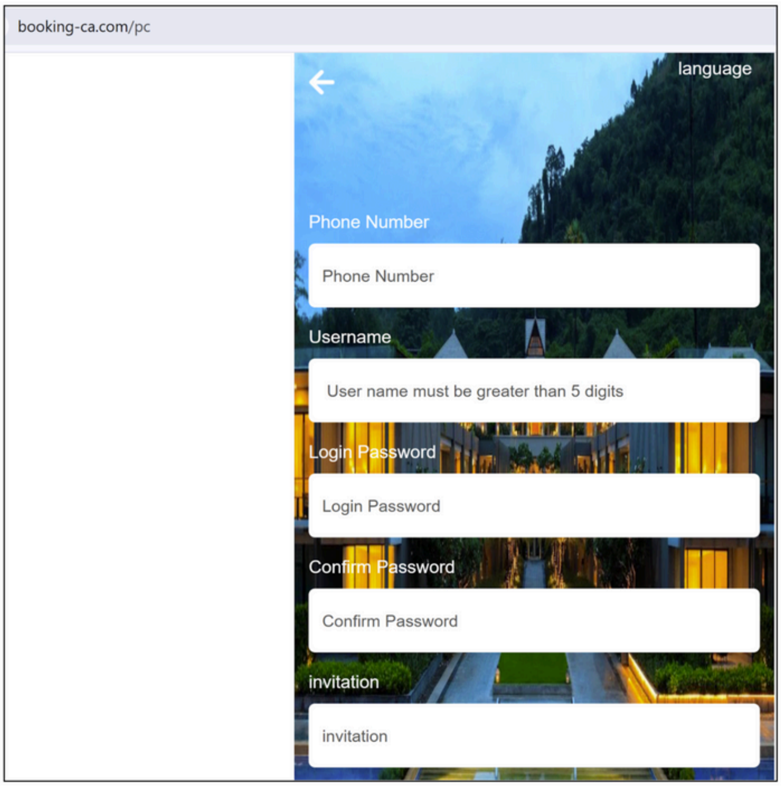
Name: Enter Name | Phone: Enter Phone | Email: Email

Show Flight

Figures 18 & 19: Typical blunders seen in the website’s content leading to doubting the authenticity

Invitation only platforms

While not novel, a method previously observed by the researchers at PreCrime Labs is the use of a multi-step phishing campaign. In the case of travel scam tactics, we identified a new website designed to target users by providing them with a private invite code to create a special, members-only account. This tactic, combined with a basic set of errors such as the website displaying only in a mobile application view even on desktop browsers and added the invite code to filter out random signups (*Figure 20*). This eliminates the risk of mass signups, ensuring users who initially believe their invite code is genuine will remain convinced of the campaign's authenticity, leading to little or no chances of detection.



booking-ca.com/pc

language

Phone Number: Phone Number

Username: User name must be greater than 5 digits

Login Password: Login Password

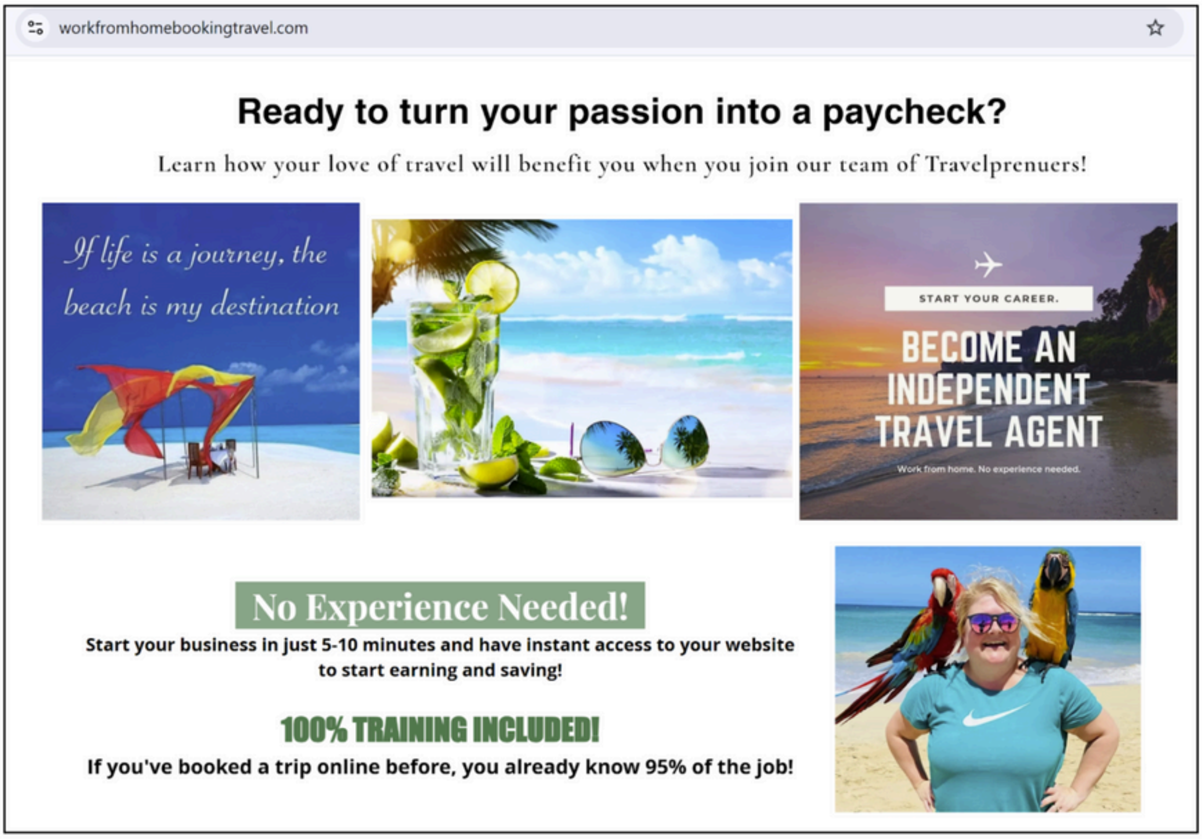
Confirm Password: Confirm Password

invitation: invitation

Figure 20: Threat actors setting up a multi stage phishing campaign with an invite only theme.

Membership websites for travel enthusiasts seeking agent roles

Numerous websites also purported to offer travel enthusiasts a "money-making" opportunity as agents through memberships. These sites typically required personal information and a "nominal" membership fee to become a "travelpreneur." Despite the questionable legitimacy of these websites, the use of keywords such as “instant” and “get-rich-quick” themes threaten to attract a lot of victims (*Figure 21*).



workfromhomebookingtravel.com

Ready to turn your passion into a paycheck?

Learn how your love of travel will benefit you when you join our team of Travelprenuers!

If life is a journey, the beach is my destination
START YOUR CAREER.
BECOME AN INDEPENDENT TRAVEL AGENT
Work from home. No experience needed.

No Experience Needed!

Start your business in just 5-10 minutes and have instant access to your website to start earning and saving!

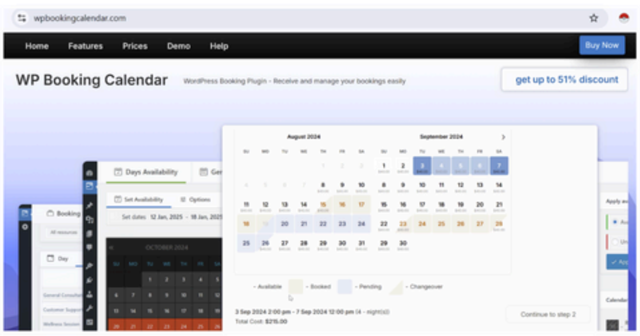
100% TRAINING INCLUDED!

If you've booked a trip online before, you already know 95% of the job!

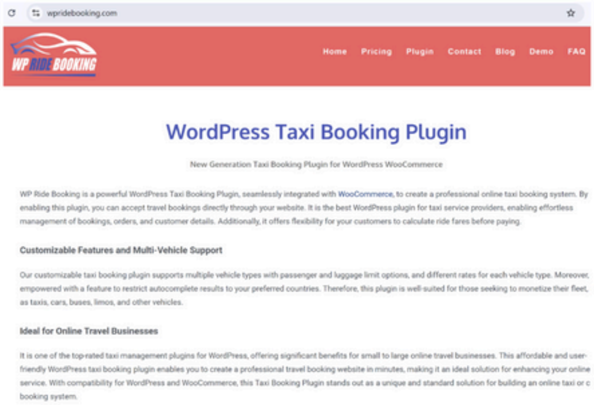
Figure 21: Get rich quick schemes to become a ‘travelpreneur’ rising during peak travel period.

Website plugins

Websites often rely on various plugins and automations to streamline their daily operations. While platforms like WordPress offer numerous plugins, researchers have recently observed paid plugins lacking online reviews or recommendations. There is a known history of cybercriminals releasing malicious plugins to steal browser credentials sessions and stored passwords. This is no different for the travel industry, where fake booking plugins were observed (*Figures 22 & 23*).



WordPress plugin for online booking and availability checking service



WordPress Taxi Booking Plugin

New Generation Taxi Booking Plugin for WordPress WooCommerce

WP Ride Booking is a powerful WordPress Taxi Booking Plugin, seamlessly integrated with WooCommerce, to create a professional online taxi booking system. By enabling this plugin, you can accept travel bookings directly through your website. It is the best WordPress plugin for taxi service providers, enabling effortless management of bookings, orders, and customer details. Additionally, it offers flexibility for your customers to calculate ride fares before paying.

Customizable Features and Multi-Vehicle Support

Our customizable taxi booking plugin supports multiple vehicle types with passenger and luggage limit options, and different rates for each vehicle type. Moreover, empowered with a feature to restrict autocomplete results to your preferred countries. Therefore, this plugin is well-suited for those seeking to monetize their fleet, as taxis, cars, buses, limos, and other vehicles.

Ideal for Online Travel Businesses

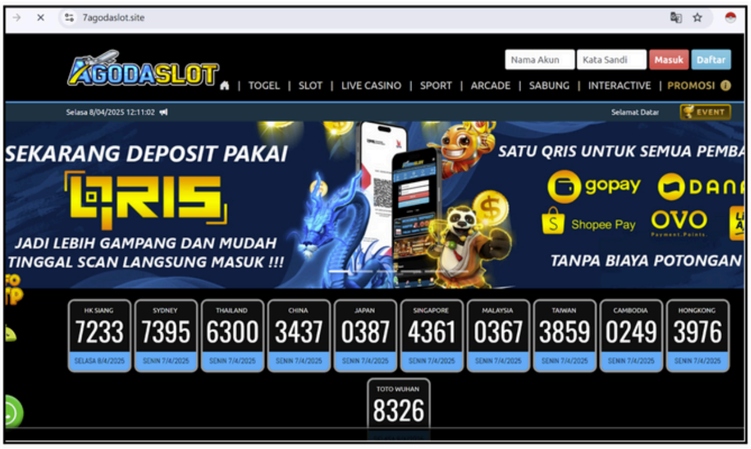
It is one of the top-rated taxi management plugins for WordPress, offering significant benefits for small to large online travel businesses. This affordable and user-friendly WordPress taxi booking plugin enables you to create a professional travel booking website in minutes, making it an ideal solution for enhancing your online service. With compatibility for WordPress and WooCommerce, this Taxi Booking Plugin stands out as a unique and standard solution for building an online taxi or c booking system.

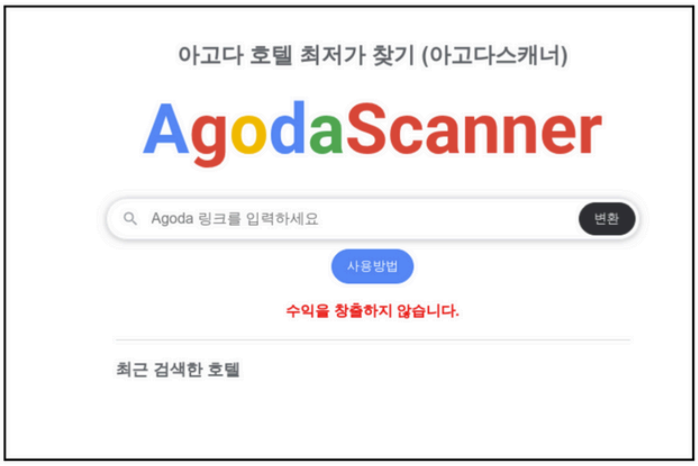
Figure 22 & 23: Newly emerged WordPress plugins need to be scrutinized for its legitimacy and intent before adding to operations

Agoda and betting

Agoda is, as we know, a popular travel aggregator. However, there's also a range of betting websites known as 'pagoda'. Since the two keywords have higher phonetic resemblance, it creates a significant risk of "agoda"-related domains being redirected to "pagoda" betting sites.

Alternatively, we also observed a website called "AgodaScanner" that is a mix of two popular OTAs, Agoda and Skyscanner. Most of the suspicious websites targeting Agoda have been in southeast Asian languages, since its headquarters and operational hub both lie in Asian countries *(Figures 24 & 25)*.





아고다 호텔 최저가 찾기 (아고다스캐너)

AgodaScanner

Agoda 링크를 입력하세요 변환

사용방법

수익을 창출하지 않습니다.

최근 검색한 호텔

Figures 24 & 25: Agoda targeted to show betting sites and generic search engines for travelling.

Individual and corporate Bookings with generic nomenclature

PreCrime Labs researchers observed an increase in domain registrations targeting corporate bookings rather than individual travelers. A case in point is the domain "skyscanner-sales," which, despite not being a fully launched phishing campaign, uses the term "sales"—a term that doesn't typically align with individual users searching for better travel deals but rather suggests corporate logins or functionalities (*Figure 26*).

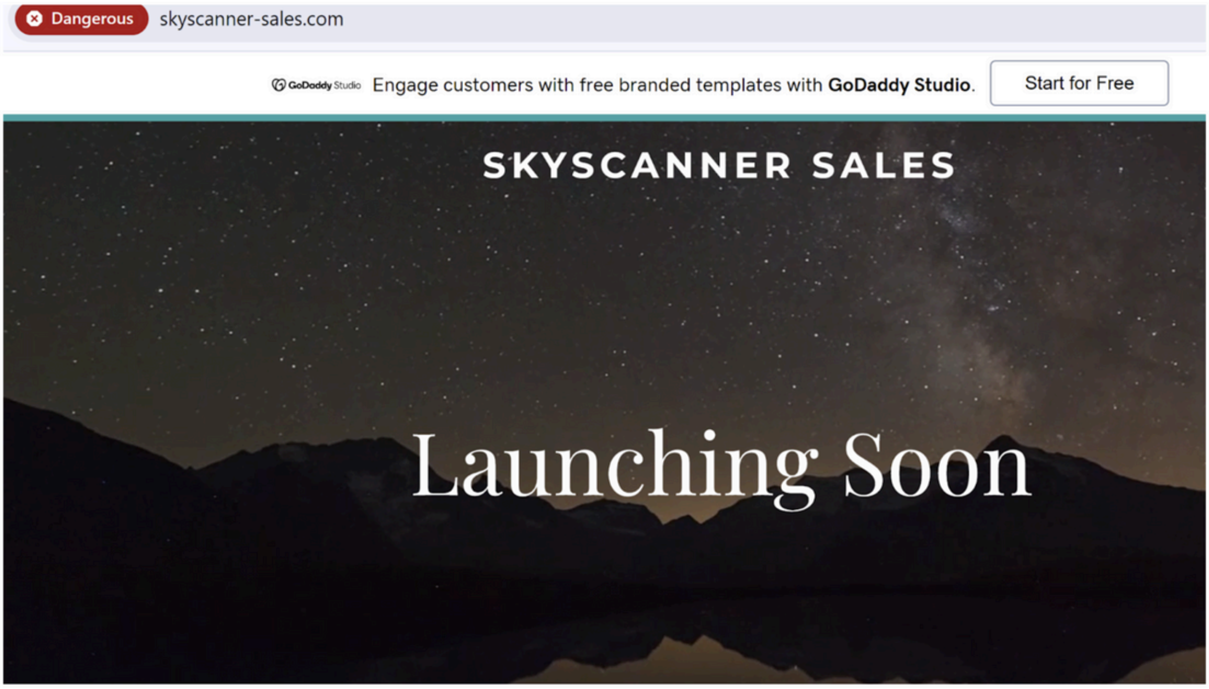
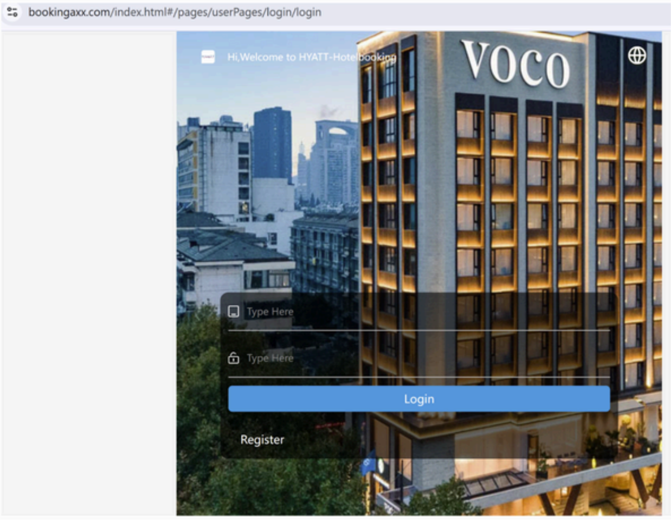
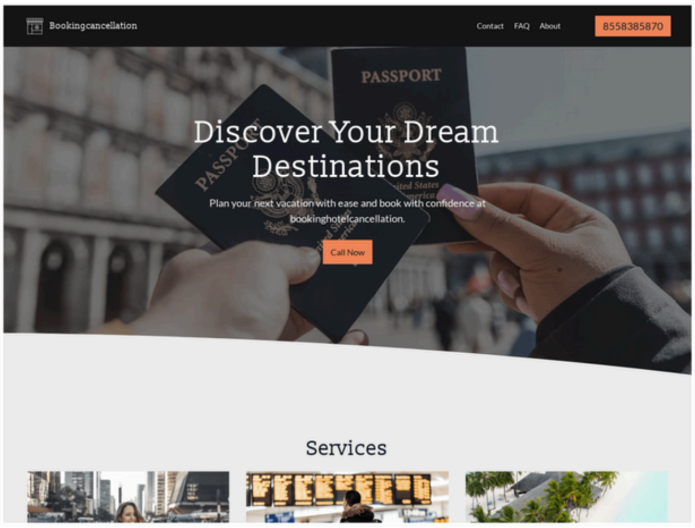


Figure 26: Phish website under construction targeting Skyscanner

Even without directly using company names, numerous domains employed generic keywords like "booking verification," "view reservations," and "approved" as their main domain, with popular OTAs listed as subdomains. This allowed threat actors to potentially collect booking details across various companies—such as Airbnb as a subdomain combined with booking-related root domains—all under a single domain (*Figures 27, 28 & 29*). This tactic was most prevalent with Tripadvisor and Airbnb.


bookingaxx.com/index.html#/pages/userPages/login/login

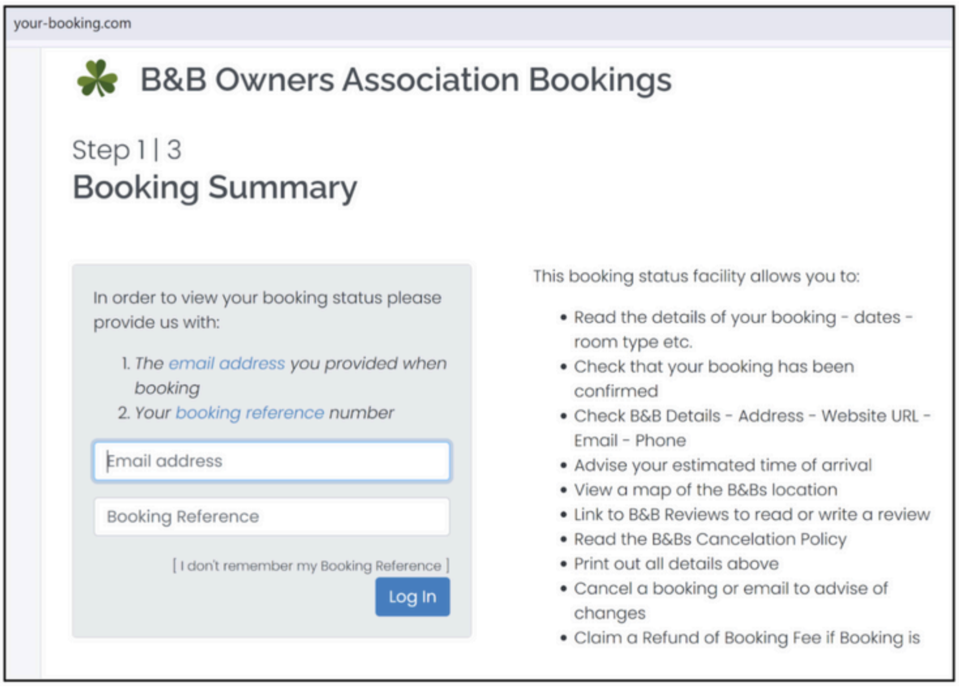
Hi,Welcome to HYATT-Hotel booking



Discover Your Dream Destinations

Plan your next vacation with ease and book with confidence at bookinghotelcancellation.

Figures 27, 28 & 29: Generic names applied while creating a root domain to host branded subdomains for phishing


your-booking.com

B&B Owners Association Bookings

Step 1 | 3

Booking Summary

In order to view your booking status please provide us with:

1. *The email address you provided when booking*
2. *Your booking reference number*

Email address

Booking Reference

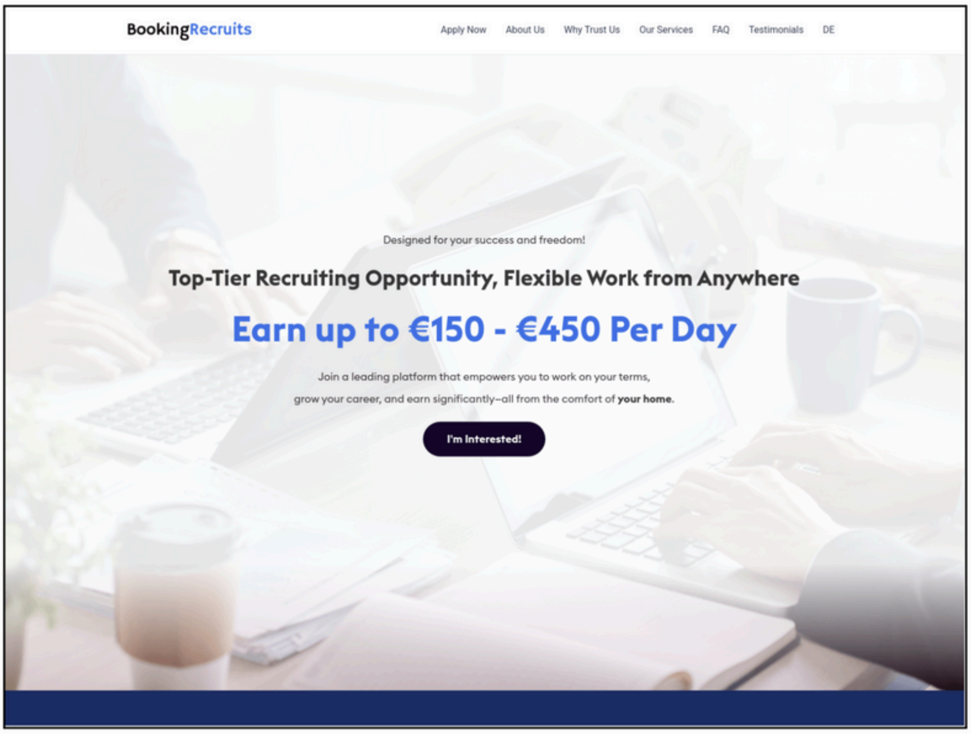
[I don't remember my Booking Reference]

This booking status facility allows you to:

- Read the details of your booking - dates - room type etc.
- Check that your booking has been confirmed
- Check B&B Details - Address - Website URL - Email - Phone
- Advise your estimated time of arrival
- View a map of the B&Bs location
- Link to B&B Reviews to read or write a review
- Read the B&Bs Cancelation Policy
- Print out all details above
- Cancel a booking or email to advise of changes
- Claim a Refund of Booking Fee if Booking is

Recruitment campaigns

Even without directly stating the company name or using its logo, different websites are attempting recruitment within the travel industry by subtly incorporating the target organization's logo theme and color schemes. For quick attention and popularity among job seekers, the threat actors might use lucrative hiring options such as ‘work from anywhere’ and attractive daily earnings, as mentioned below (Figure 30).



Designed for your success and freedom!

Top-Tier Recruiting Opportunity, Flexible Work from Anywhere

Earn up to €150 - €450 Per Day

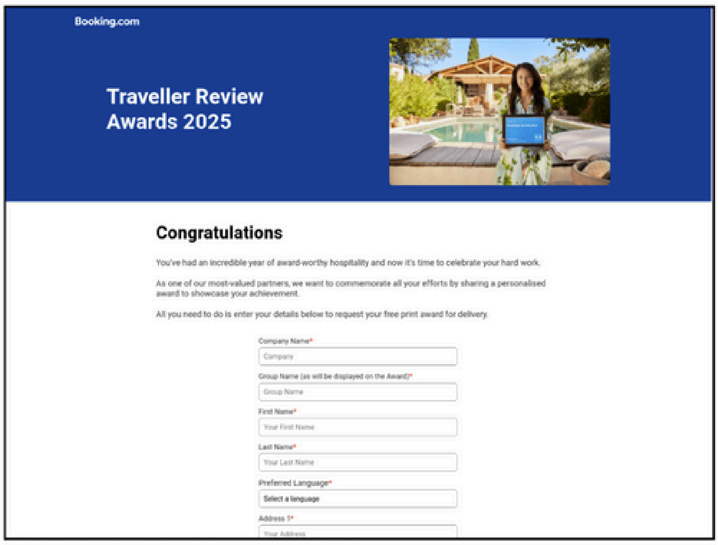
Join a leading platform that empowers you to work on your terms, grow your career, and earn significantly—all from the comfort of **your home.**

Figure 30: Recruitment phish pages appearing during the peak in travel season.

Fake corporate awards/rewards

Beyond targeting individual travelers, threat actors also see a larger opportunity in corporate annual rewards and awards programs. In one such instance, Booking.com, a popular flight and hotel aggregator, was impersonated to offer awards to other companies. Further, for the winners to get free delivery, personally identifiable information (PII) was requested. This indicates a targeted attack, focusing on specific employees within companies rather than the general traveling public, indicative of a sophisticated phishing operation.

Alternatively, for individuals, there’s always a coupon system that has a higher chance of succeeding as phishing attempts. Given below is an example, where the website offers a wide range of travel coupons despite lacking proper contact information, likely targeting anyone seeking a good travel deal (Figures 31 & 32).



Booking.com

Traveller Review Awards 2025

Congratulations

You've had an incredible year of award-worthy hospitality and now it's time to celebrate your hard work.

As one of our most-valued partners, we want to commemorate all your efforts by sharing a personalised award to showcase your achievement.

All you need to do is enter your details below to request your free print award for delivery.

Company Name*
Company

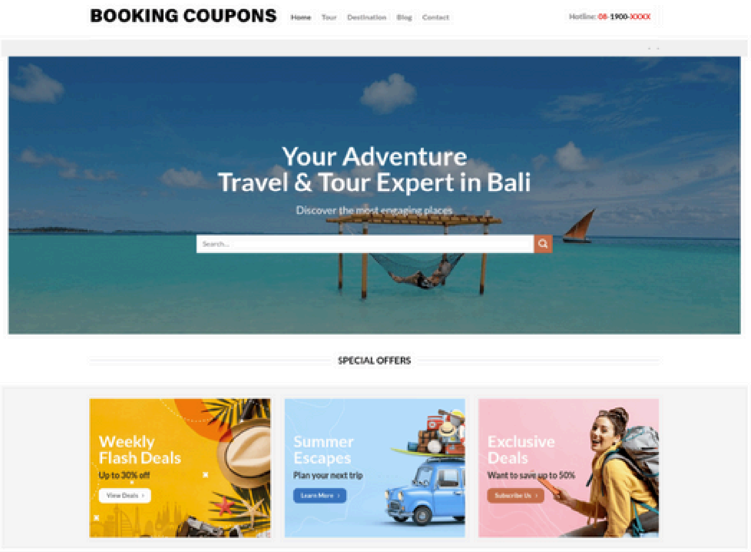
Group Name (as will be displayed on the Award)*
Group Name

First Name*
Your First Name

Last Name*
Your Last Name

Preferred Language*
Select a language

Address 1*
Your Address



BOOKING COUPONS

Hotline: 08-1900-XXXX

Your Adventure
Travel & Tour Expert in Bali

Discover the most engaging places

Weekly Flash Deals
Up to 30% off

Summer Escapes
Plan your next trip

Exclusive Deals
Want to save up to 50%

Figure 31 & 32: Awards and rewards theme used to phish corporations as well as individuals.

Conclusion and mitigation

As is demonstrated in the above observed domains, that while a gradual transition is seen where malicious travel campaign activity has slowed, it has not, and will not, stop.

Furthermore, while rewards and employee-focused domains target specific groups, they represent a consistent threat landscape.

In the case of the hotel industry, BforeAI's Indicators of Future Attack (IoFA) platform demonstrated high efficacy in preemptively identifying malicious domains, capturing over 85% before content activation. This predictive capability is attributed to the analysis of signals such as the use of parked brand terms combined with generic keywords, recent registration with low-reputation hosters, and patterns aligning with established campaign infrastructure. For instance, the domain zerofeesairbnb[.]com was registered just one day prior to its activation within a Telegram-based scam operation.

For individuals engaging with any website from the travel and hotel industry, should be careful by observing simple and easy to identify red flags.

1. The web browser may often flag suspicious sites that should be avoided.

2. Website with the same thematic content as the legitimate one, but has a different logo or irrelevant content.

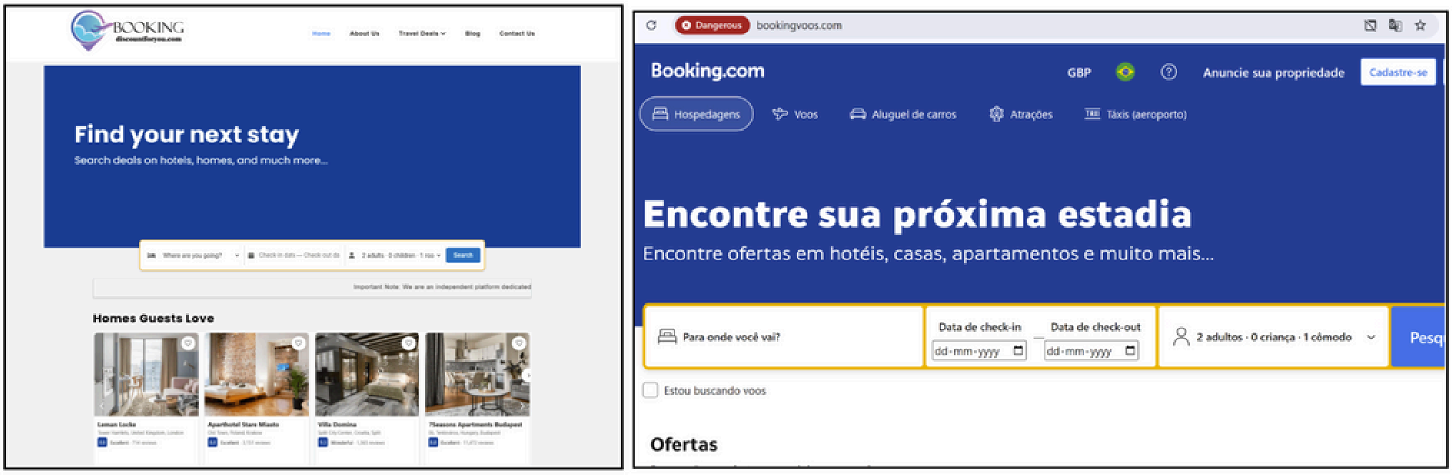
3. Broken links, distorted reference pictures, gaps in features, or any added functionality which is uncommon for travel websites.

4. Check for deals too good to be true, as peak travel season means inflated discounts disguised as lure baits.

5. To prevent widespread compromise, avoid using the same passwords across multiple aggregation sites.

6. Avoid clicking on invite codes without thoroughly verifying the associated websites.

7. Finally, individuals working in travel companies should be vigilant regarding training sites, employee logins, and verification portals that could be attempts to steal their corporate credentials.



Find your next stay

Search deals on hotels, homes, and much more...

Important Note: We are an independent platform dedicated

Encontre sua próxima estadia

Encontre ofertas em hotéis, casas, apartamentos e muito mais...

□ Estou buscando voos

Figure 33 & 34: Reference for individuals to beware of phishing campaigns.