OMNI HOTELS & RESORTS®

Testimony of

Ms. Jamie Pena, Vice President of Revenue Strategy & Global Distribution

Omni Hotels & Resorts, Dallas Texas

Before the House Energy & Commerce Committee

Subcommittee on Commerce, Manufacturing and Trade

On H.R. 4526, the "Stop Online Booking Scams Act"

Introduction

Chairman Burgess, Ranking Member Schakowsky and members of the Subcommittee on Commerce, Manufacturing and Trade, thank you for the opportunity to speak to you today about how Congress can address the growing problem of deceptive hotel booking websites. My name is Jamie Pena and I am Vice President of Revenue Strategy & Global Distribution for Omni Hotels & Resorts based in Dallas, Texas. I also reside in Texas's 26th Congressional District, so I am a proud constituent of yours, Chairman Burgess. Currently, I serve on the American Hotel & Lodging Association's Consumer Innovation Forum, which is made up of the industry's digital marketing and distribution executives and focused on issues arising from the changing online digital marketplace and how to ensure we continue to serve our guests in the best way possible.

It is an honor to appear before your committee today to share with you Omni's experience working to prevent consumer deception and fraud in online hotel bookings and the need for Congress to pass the "Stop Online Booking Scams Act, H.R. 4526." On that note, I would like to thank the sponsors of the SOBSA bill: Representatives Frankel, Ros-Lehtinen, Shuster, and the fourteen other bi-partisan cosponsors for their leadership on this issue. They recognize the importance of ensuring that everyday consumers are not left holding the bag because unscrupulous actors have figured out a way to manipulate the system. We commend them for their efforts.

By way of background, Omni is a luxury hotel brand with 60 hotels in North America, boasting over 18,000 associates in the United States, Canada and Mexico. We pride ourselves on creating memorable, unique experiences for every guest by exceeding their expectations while inspiring and rewarding our associates.

Omni Hotels and Resorts is a proud member of the American Hotel & Lodging Association (AH&LA), the sole national association representing all segments of the 2 million-employee U.S. lodging industry, including hotel owners, REITs, chains, franchisees, management companies,

independent properties, bed and breakfasts, state hotel associations, and industry suppliers. With over 23,500 properties in membership nationwide, the AH&LA represents more than half of all the hotel rooms in the United States.

I have 24 years of experience in the hospitality industry across multiple disciplines with both ownership groups and brands. My tenure with Omni began in 2009 and my current responsibilities include overseeing all revenue management and distribution for the brand. This oversight includes negotiating partner agreements; sourcing and managing technology to distribute our rates and availability and enduring parity across all points of sale including voice reservations.

Deceptive Hotel Booking Websites Are Harming Consumers

H.R. 4526 is targeted to address scam websites that are taking advantage of new advances in online booking technology. The ever-evolving online channels for booking hotel rooms, from desktops to mobile phones to internet-enabled devises like smartwatches, have transformed the way guests book their hotel rooms and created new customer-oriented business models. Amid these transformations, the lodging industry continues to put guests first. We are focused on educating consumers on how to protect their reservation and ensure their experience is beyond their expectations.

It is with this perspective that we bring to the Committee a growing problem of misleading scam websites that deceive consumers into thinking they are making a legitimate booking directly with the hotel company. These websites are designed to look and act like a hotel website, but are not. They use pictures and graphics, and other unique images from the hotel. They set up 1-800 number call centers, and when the potential guest calls, the reservation agent answers in a way that makes the consumer think that he or she is speaking directly with the hotel or brand. Further, as consumers increasingly move to mobile booking, smaller screens make it even more difficult for consumers to differentiate between a scam site and the legitimate hotel website, as URLs and other key indicators,

are hidden. These scams result in a host of consumer complaints, including lost reservations, incorrect accommodations, loss of hotel reward points, and clear consumer confusion. By AH&LA's estimates, these scams are impacting up to 15 million online hotel bookings a year.

Examples from Omni Hotels & Resorts Include:

The Omni Parker House in Boston recently had a guest call to add an additional guest name to their reservation that she booked online. The agent was unable to assist the guest because they had unknowingly given their payment information to a third party. The guest was very upset that her credit card information was in the hands of "strangers" since she thought she booked directly with the hotel. This particular guest confirmed that the link she clicked on contained the word "Omni" so she assumed it was our brand site.

The Omni Houston Hotel had a similar scenario occur recently when the guest realized they had clicked on a link that they believed directed them to Omnihotels.com, but to the guest's surprise, it did not. She ended up booking through a third party unknowingly. She only realized several days later that this happened when the agency called her back and said they found a cheaper rate at another brand hotel nearby. In this instance, she called to alert the hotel manager that this happened and to ensure she would still receive her Loyalty Program benefits. I personally called this agency's phone number anonymously and the agent continued to insist that he was an agent of Omni Hotels.

Both our Atlanta CNN hotel and our Amelia Island Resort have had instances of email phishing scams where a third party will send email blasts to membership groups meeting at the hotel in an attempt to direct them to a third party website to book their sleeping room reservation for a meeting or convention. This is particularly deceptive because the emails appear very official and reference the organization and event by name.

This isn't just a problem for customers trying to book with Omni Hotels. Below is just one of a growing number of examples of these deceptive sites affecting consumers around the country. Below

is an example of a deceptive website, which to the consumer looks like the website for the actual property.

mccarren-hotel-brooklyn.h-rzn.com/index.htm?lbl=gglrmk

HR McCarren Hotel & Pool

Secure Hotel Reservations ★★★★ 160 N 12th St, Brooklyn, 11249, NY, United States

BOOK ONLINE OR CALL
US: +1 800 299 9572
UK: +44 203 564 5666
EU: 00 800 4321 1111

Hotel Info | Rooms | Photo album | Area information | My booking | Contact us | English | USD ($)

BOOK ONLINE NOW

CHECK-IN DATE 10 Apr 2015 Friday
CHECK-OUT DATE 11 Apr 2015 Saturday
1 Night

ROOMS 1 | Room 1 | ADULTS 2 | CHILDREN 0

CHECK RATES

Rates from USD 226

HOTELS IN UNITED STATES » HOTELS IN BROOKLYN

McCarren Hotel & Pool is a luxurious 4-star property in Brooklyn.

Accommodation
The hotel offers 64 comfortable and well-equipped guestrooms. **Beds**: Rooms at McCarren Hotel & Pool boast premium bedding. **Bathroom** amenities include bathrobes, complimentary toiletries and designer toiletries. **Entertainment**: In-room entertainment options at McCarren Hotel & Pool include flat-screen TV. Housekeeping services are also available.

Facilities
McCarren Hotel & Pool is a smoke-free property. Dining facilities at the hotel include a restaurant. There is also room service available. The hotel boasts a 24 hour front desk service. Other hotel amenities include tennis court(s). **Leisure**

Make no mistake, these sites are designed to deceive the consumer.

Educating Consumers Is One Important Step

Thankfully, the hotel industry is one of many voices concerned about this growing problem and we are grateful for those who are working with us to address it. AAA and the Better Business Bureau, two noteworthy consumer protection organizations, have issued alerts to their members on the rise of these scams which included information on how to protect themselves. The Federal Trade Commission (FTC or "Commission") also issued two alerts last year, focused on both leisure and

business travelers. We truly appreciate our partnership with the Commission and these associations. We also submit for the record letters of support from Ashford Hospitality Trust, another Dallas-based hotel company, as well as multiple state lodging associations including the Florida Restaurant and Lodging Association, the North Carolina Restaurant and Lodging Association, the Texas Hotel and Lodging Association and the Conventions Industry Council.

Our industry is also working to develop better methods of tracking the expansive nature of the problem. All too often, instances of fraud do not get reported because the front desk of the hotel will go out of its way to accommodate the victim of the deceptive website. So, in many of these cases the problem does not get reported to hotel management. That is why our industry is beginning a pilot program in 3 states (Arizona, Iowa, and Mississippi) to train front desk personnel on how to report instances of fraud directly to state attorneys general offices. We will continue to keep the Committee and the FTC updated on our findings.

The issue has also been highlighted in multiple news articles, magazines, and television shows, including ABC Nightline, New York Times, and L.A. Times.[1] Unfortunately, consumer education is proving not to be enough. As the number of consumers booking hotels online continues to rise, especially in the mobile space, so will the instances of deceptive sites.

Stop Online Bookings Scams Act (H.R. 4526) Is A Targeted Solution

That is why I am here today to express our support for H.R. 4526, the Stop Online Booking Scams Act. This bipartisan legislation will help protect consumers from these online hotel booking scams by prohibiting websites from pretending that they are an actual hotel. Importantly, for those consumers who are scammed, the bill allows for the state attorneys general to pursue damages and

[1] Attached as Exhibit A are just a few examples of consumer alerts, articles, blogs, and links to videos highlighting the problem.

restitution on behalf of victims. This will help make consumers whole while also serving as a significant deterrent to potential bad actors.

The Stop Online Booking Scams Act is narrowly tailored to address only those unscrupulous websites that purposefully deceive the consumer. The legislation excludes our partner Online Travel Agencies (OTA's) that are "affiliated," or have direct relationships, with hotel companies. While no one should be given a free pass when it comes to deceiving customers, we have found that OTAs that have direct relationships with hotels tend to design their websites in a manner that distinguishes their site from the hotel. In addition, because hotels have a direct relationship with these sites, the hotel and website operator can typically have a one-on-one conversation to address any instances of confusion. In my experience, these occasional instances are handled quickly as both parties are eager to have a mutually beneficial relationship.

Further, most OTAs that have direct contracts with hotel companies already display in a conspicuously visible manner that they are not the actual hotel. Mainstream OTA's are all conspicuously branded and clearly show the consumer through graphics and logos that they are not the actual hotel property. The bill's intent is to go after those truly rogue scam websites that are clearly designed to deceive the consumer.

I thank the Committee for inviting me to testify today on this important consumer issue, and I am happy to answer any questions you may have.

EXHIBIT A

FEDERAL TRADE COMMISSION
CONSUMER INFORMATION
consumer.ftc.gov

Did you book that night at the hotel's site?

July 14, 2015
by Amy Hebert
Consumer Education Specialist, FTC

Whether you travel a lot or just a little, you've probably gone online to book a hotel stay. Sometimes you might find a travel comparison site gets you the best deal. Other times, you might book directly at a hotel's website — maybe to earn points for the company's reward program, or because you have some special requests for your stay.

For those times you're looking to book directly with a hotel, make sure that's what you're doing. The FTC has heard from people who searched online and thought they were booking on a hotel website, only to find they'd unknowingly been doing business with someone else.

The confusion resulted in problems like:

- arriving and finding no reservation
- having trouble canceling or modifying a reservation, or disputing charges through the hotel
- finding reserved rooms didn't reflect special requests like disability access
- being charged undisclosed fees
- paying a higher rate than what's advertised by the hotel
- getting credit card charges from the third party, not the hotel
- not earning points with their hotel reward program

It can be hard to tell that you're not on the hotel's site. You might see a hotel's name in the URL, or call the number shown next to the hotel's address and not realize it's the reservation company — not the hotel — you're talking to.

Your best bet to avoid surprises — look closely at your search results. If you know you want to deal directly with a hotel, take the time to look for signs you might be on a third-party site, like another company's logo. It's also a good idea to find the hotel phone number yourself, rather than rely on what's listed on the site.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Business travelers: Check it out before you check in

Lesley Fair
Jul 14, 2015

TAGS: Human Resources | Non-Profits | Bureau of Consumer Protection | Consumer Protection | Advertising and Marketing | Advertising and Marketing Basics

Here's a tip for business travelers. Just because a webpage looks like the official site of your favorite hotel chain doesn't necessarily mean it is. Before you reserve a room for your next out-of-town meeting or family vacation, make sure you know who's at the other end of that BOOK NOW button.

The internet offers savvy travelers lots of options for getting the best deal on hotels. You can contact a property directly, book through a hotel chain's website or toll-free number, visit one of those travel comparison sites, or use a third-party online hotel reservation service. The choice is yours – but make sure it's an informed choice. Some third-party sites clearly disclose that they're not affiliated with the hotel. Others appear to mimic the look of a chain's official site, making it tougher for consumers to know who they're doing business with.

Why would it make a difference to travelers? According to some reports, people have arrived at their destination only to find there's no record of a reservation in their name. Another concern: Reservations made through a third-party site may not count toward a hotel's rewards program. In other instances, special requests made through a third-party site may not be conveyed to the property where you'll be staying. Another potential risk is that third-party sites could have policies about things like pre-payment, cancellations, or refunds that differ from the chains you're used to dealing with directly.

How you decide to book a room for your next trip is up to you, but getting the straight story about who's handling the reservation isn't always easy. If you type a hotel name into a search engine, it's unwise to assume that the first result that pops up will always be the official site. Some third-party reservation companies pay for the top spot on the results page or buy prominent space on the right.

What about looking for the names, logos, or URLs of familiar chains? Some third-party sites look a lot like the official sites, so you can't rely just on the usual visual cues. Calling a number listed online can be problematic because some third-party sites use call centers that are hard to distinguish from a chain's official reservation line.

What steps can a traveler take to be better informed?

- If it's important to you to book directly through the hotel chain, consider using the toll-free number or URL on your rewards card or featured in the company's TV or print ads.

- Whether you choose to book through a chain or through a third-party site, read the details carefully with an eye out for any fees or surcharges that may lurk in the fine print or behind vaguely labeled hyperlinks.
- If you received an email confirmation, travel with a printed copy or have it easily accessible on your smartphone.
- Before you hit the road, use a number you know to be genuine to call the hotel directly. Double-check that your reservation is in the system.
- Share these tips with your company travel office or anyone else who makes reservations on behalf of your business.

ftc.gov

Council of Better Business Bureaus

Change Location

Scam Alert -- Booking a Hotel This Summer? Don't Fall This Scam

Like Share 64 G+ Share 2 Share 4 Tweet

May 26, 2015

Taking a vacation this summer? Be extra careful when booking accommodations online. Fake websites appear to offer travelers a convenient way to reserve hotel rooms, but they are just making money for scammers.

How the Scam Works:

You are planning a trip and need to book a hotel room. You see an online ad promoting hotel rooms at a cheap price, and you click it. You are directed to a website that looks legitimate. It may have a URL similar to the real hotel website or established third-party booking site, such as Hotels.com or Expedia.com. The website may also use the same logo, colors and/or design of the legitimate site.

The website might look okay, but it's a fraud. Scammers are creating fake hotel booking websites to steal money from travelers. Some scam sites make money by tacking on additional fees, but others charge you for a room that simply doesn't exist. In any case, sharing your credit card and personal information (such as name, address and phone number) on scam websites puts you at risk for identity theft.

How to Spot a Fake Website

Here's how to spot a fake website:

1. **Don't believe what you see:** The site may have the logo or design of a legitimate hotel or booking site, but that can be easily copied from the real website.
2. Look out for fake contact info: Some consumers report calling the 1-800 number posted on a scam hotel booking site to confirm its legitimacy. Scammers simply impersonated the front desk of the hotel.
3. **Double check the URLs**. Scammers pick URLs that look very similar to those of legitimate sites. Always be sure to double check the URL before making a purchase. Be wary of sites that have the brand name as a subdomain of another URL (i.e. brandname.scamwebsite.com), part of a longer URL (i.e. companynamebooking.com) or use an unconventional top level domain (brandwebsite.net or brandwebsite.co)
4. **Look for a secure connection.** Make sure your personal information is being transmitted securely by ensuring the web address starts with "HTTPS" and has a lock icon.
5. **Watch for too good to be true deals**. Be sure to comparison shop and be suspicious of a site that has prices significantly lower than those listed elsewhere.

For More Information

To learn more, check out this alert and infographic (http://www.ahla.com/OnlineHotelBookingScams/) from the American Hotel and Lodging Association. To find out more about other scams, check out BBB Scam Stopper (bbb.org/scam (/council/bbb-scam-stopper/)).

NOTE: Hotels.com and Expedia.com are BBB Accredited Businesses.

WESTERN UNION (http://www.westernunion.com/Home)

moving money for better

This Scam Alert has been sponsored by Western Union, a BBB National Partner.

BBB Directory (/bbb-directory/)

Give.org (http://www.give.org/)

Contact (/council/about/contact/)

BBB Business Partner Code (/bbb-business-partner-code-of-conduct/)

BBB API (https://developer.bbb.org/#/)

Your Ad Choices (/council/about/privacy-policy/#adchoices)

Terms of Use (/council/about/terms-of-use/)

Trademarks (/council/about/trademarks/)

Privacy Policy (/council/about/privacy-policy/)

Fight Phishing (/council/consumer-education/fight-phishing/)

Select Language | ▼

© 2016 Council of Better Business Bureaus

The Washington Post

Travel

When should you have reservations about your hotel reservations?

By Christopher Elliott Columnist May 14, 2015

When it comes to booking a hotel online, what you see isn't always what you get.

Christina Daves knows. On several occasions, she's shopped for a hotel room online and then clicked through to make a reservation, only to discover she was actually dealing with a third-party site that looked like a hotel site.

"Often," said Daves, who owns a medical device company in Washington, D.C., "there are no refunds on a reservation made through one of these sites, if you want to cancel or make a change."

The hotel industry is worried, too. It recently asked the Department of Justice to investigate travel sites that are "trying to pass themselves off as the actual hotel." The industry, represented by the American Hotel & Lodging Association (AH&LA), estimates that 2.5 million bookings are affected by this site-spoofing each year, which translates into more than $220 million going toward what it calls "bad" bookings.

At best, these reservations are simply made on behalf of a third party instead of by the hotel and may have additional restrictions or booking fees. But at worst, they may be completely bogus bookings that won't be recognized by a property.

Pinpointing the problem is easy, but a solution isn't. It turns out the fake sites operate outside the country and can be difficult to identify as fraudulent.

Who are these companies? There are thousands of them, according to AH&LA, and they go by names like Reservationcounter.com, Reservationdesk.com and Hotelsone.com.

"These sites are constantly changing their names, URLs and phone numbers to evade legal repercussions," said Maryam Cope, AH&LA's vice president of government affairs. "If you go to one of these sites, the phone number will likely be one thing around 3 p.m. and something else by 6 p.m., then again something else by 10 p.m. It's a constant cat-and-mouse game to keep up with these rogue sites."

Hotelsone.com did not immediately reply to a request for comment. Daniel Nelson, the chief executive of TravelPASS Group, the Salt Lake City-based company that operates the sites Reservationcounter.com and Reservationdesk.com, said his company's sites have been around for many years and that reservations made through them are legitimate. He denies they are trying to imitate hotel Web sites, which is obvious when you compare the sites.

"The AH&LA is trying to turn this into a 'buyer beware' story," he said. "But the truth is, if they get their way — if the only safe booking is a direct booking — it will limit consumer choice and reduce your options."

Indeed, there's more happening here than meets the eye. It's a barely visible conflict between hotel operators and the online agencies, many of them legitimate, which help them sell their inventory. They seem to be waging a war of rhetoric, using anecdotes as ammunition. Consumers are caught in the crossfire.

Merle Kappelmann, who owns the Flamingo Inn in Daytona Beach, Fla., said she was taken aback when seven guests walked into her hotel during the city's annual Bike Week and claimed to have reservations at $79 a night. They didn't. Rooms were going for between $179 and $200 per night that week, and she could find no record of the group. The reservation had been made by a mysterious company named Reservation Counter, she said.

"We called and asked, 'How is it possible that they can have our information available for people to make reservations without us signing a contract or agreeing to rates?'" she recalled. "They were unable to give us answers and refused to tell us where they were located, who owns the business, and since they all had foreign accents, we thought they may have been out of South America."

To further complicate the issue, some sites that appear to be trying to capitalize on a hotel's name are actually legitimate. Greg Fisher, the president of a regional online travel agency called TripShock, says his hotel listings in the Florida Panhandle show up on Internet search engines before the actual hotel, which may lead some inexperienced travelers to believe they're clicking on a hotel site. Still, the reservations they make through his site are valid.

"I do believe it's mostly a generational problem," he said. "Most people will be aware. But it's still something we deal with weekly."

One of the most enduring "wrong site" examples is the National Park Reservations site, which is sometimes confused with the National Park Service site by consumers. It isn't affiliated with the national parks, a fact that it now clearly discloses on its front page, and it charges a fee for reservations made through the site.

It's the first result on Google for a "national park reservation" search, but the site most people actually want is NPS.gov (go to "Find a Park"), which doesn't have the fees. You can also book national park reservations, minus the fee, via an authorized concessioner such as Xanterra reservations.

Hotels are fighting these third-party sites not just because of the customer confusion but also because they would prefer to take your reservation directly, without having to pay a commission. But their advice is still reliable. Take a hard look at the site before you book; otherwise, you could end up paying more or booking an invalid reservation.

"Make sure you know who you are dealing with," Cope said. "Third-party vendors often make promises they can't keep, and they likely can't help if something goes wrong."

Cope said even calling the 800 number isn't a reliable way to verify a site's identity, because the rogue sites claim to be the hotel's reservation desk.

"You really need to be careful," she added.

If you've been scammed by a fake hotel site, contact your credit card company immediately to initiate a dispute and then get in touch with the Federal Trade Commission to file your complaint. Because chances are, this problem will get worse before it gets better.

Elliott is a consumer advocate, journalist and co-founder of the advocacy group Travelers United.
E-mail him at chris@elliott.org.

Travel newsletter
A weekly tipsheet for those who love to get away.
Sign up

More from Travel:

Travel Guide

Ski Guide

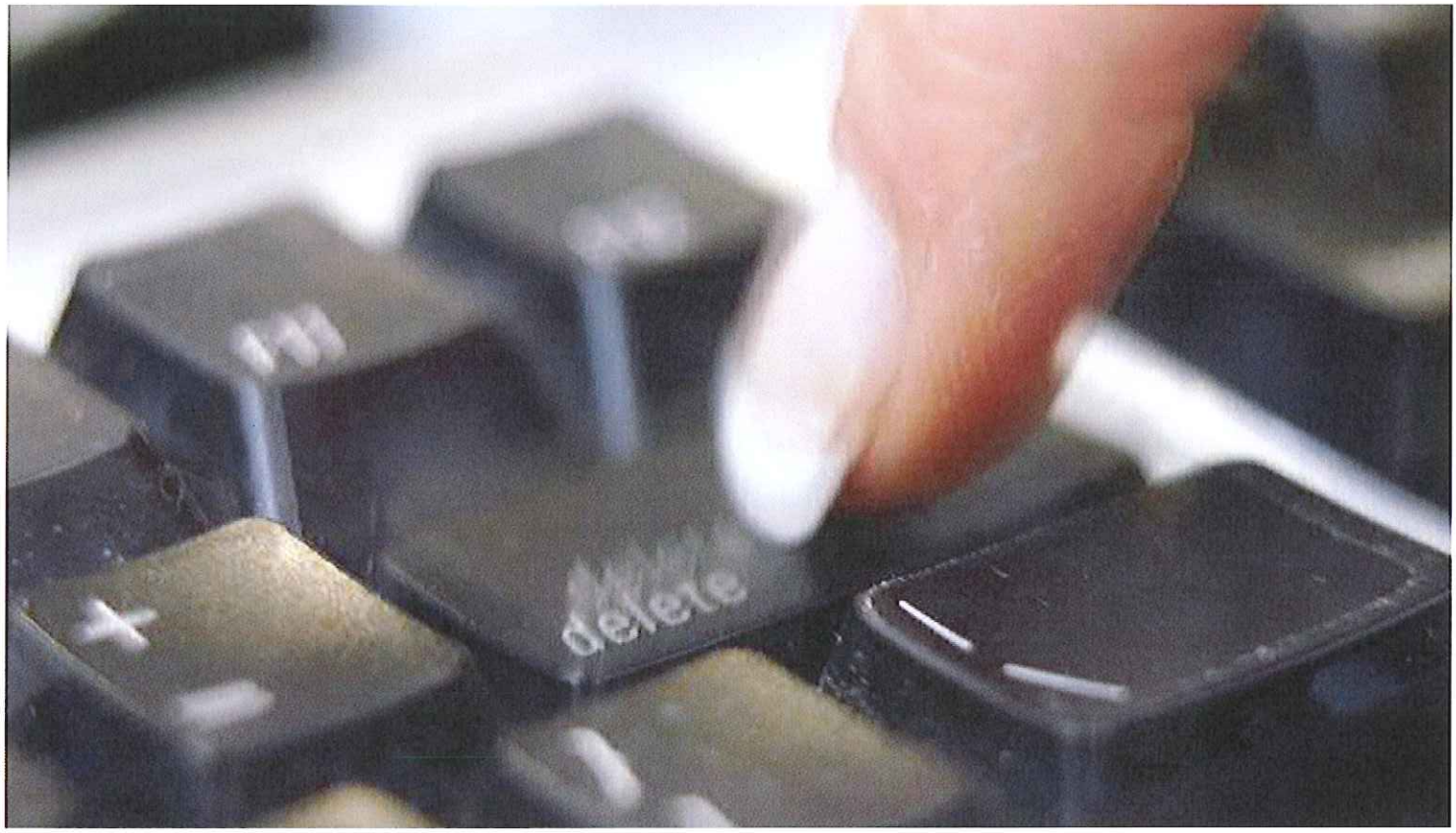
Caribbean Guide

Read more from Travel:

Read past Navigator columns here

TRAVEL / Travel News & Deals

How crooks try to hook you into scam hotel bookings



Kirk McKoy / Los Angeles Times

By **Catharine Hamm · Contact Reporter**
On the Spot

JUNE 15, 2015, 7:30 AM

Pay attention or pay the price. That's the bottom line on an online hotel-booking scam that's recently caught the attention of a U.S. senator who has asked the Federal Trade Commission to look into these insidious schemes.

This isn't a new hoax, but it has recently come to the attention of Sen. Chuck Grassley (R-Iowa), who has expressed his concerns in a letter to the FTC. In it, he noted that duplicitous third-party booking sites, which dress themselves up to look like legitimate sites, get people to book.

If they get rooms — and they often don't — consumers who arrive at the hotels may not have the

amenities they requested or, worse, necessities such as a handicapped-accessible facilities.

And, most critically, their payment details may have been exposed.

The FTC could not provide me with information on what steps it might take to address the concerns Grassley outlined.

But the issue represents a huge threat to the consumer.

"In North America, about 480 hotel bookings are made online every minute," said Maryam Cope, vice president of governmental affairs at the American Hotel & Lodging Assn., whose figures show that about 2.5 million bookings a year may be affected.

The scam involves many variations on "phishing," designed to get you to divulge personal information. Most familiar is the email that tells you about a great deal on hotel rooms. All you have to do is click a link. (Don't.)

Or you might search for "hotel rooms in XYZ City" and up pops a site that looks like the site of a chain you know and trust — but it isn't that site. You're busy so you don't notice that something is not quite right. (Are there extra words in the URL? A legitimate site is usually ItsName.com.)

Or a hot tip could come through social media. "It's taking advantage of trust," said Scott Olson, vice president of product for Iovation, a device-based fraud intelligence company. (Would your friend recommend a hotel chain? Really? Think about getting more interesting friends.)

The crooks are becoming increasingly sophisticated, tech and travel experts say.

"It's easy for someone to 'skin' another company's website to create a phishing website," said Henry Harteveldt, founder of Atmosphere Research and a travel analyst. The bad guys are "basically taking the look and feel and copying, in some cases with an alarming amount of accuracy." But, he added, there's "no real content, no real functionality.... All [the site is] doing is capturing your personal information."

These phony sites are especially hard to detect on mobile devices, whether smartphone or tablet, on which the type tends to be smaller or harder to read. Thus you may not notice that there's something fishy about the URL, which may include another name along with the legitimate hotel name.

That's alarming because mobile represents about a quarter of travel bookings, said Umar Riaz, managing director of the hospitality and travel services practice at Accenture, a management consulting firm.

One saving grace, Riaz said: You're more apt to use a legitimate app on mobile.

Even if you're among the people who use a PC or desktop to book travel, you may not be accustomed to looking at sites closely. Here are some clues that the site is a scam:

Spelling, punctuation or grammatical errors.

Missing a "lock" in the left side of the address bar. "Ensure that the website you are visiting supports 'https' when booking hotels, shopping or entering any type of personal information," said Ondrej Krehel, chief technical officer and founder of LIFARS, a cybersecurity intelligence firm based in New York City. You'll know you are connected by https if you see a lock in the URL bar of your Web browser.

Unfamiliarity. You don't recognize the site or you haven't done business with it. About 30% of users will use a search engine asking for "hotels in San Francisco," for instance. That can be dangerous, Riaz said, because it opens you up to a fake site. Better to go through an established hotel site such as http://www.marriott.com or use an online travel agency such as Expedia or Travelocity, or an aggregator such as Kayak or Hotels.com.

Too good to be true. Be especially wary if the fabulous offer arrives in your email. If you're offered the Four Seasons Maui for $200 a night, hit delete. (I checked random dates in July for that property in Wailea and it starts at $639 a night, its for-real website said.)

Also be afraid if the email uses an odd salutation. (I just found an email in my spam folder that begins, "Good day to you." Besides the fact that no one talks that way anymore, it also was purportedly from Jack Lew, who wants to send me $10 million. He probably has more important things to do in running the Treasury Department than to notify me of this inheritance.)

A button that gives you a phone number (or, on mobile, connects you) to the "hotel." If you decide to call, ascertain whether it's legitimate by asking lots of questions. For instance, how many rooms does the hotel have? How far is it from the airport? What shopping is nearby — ask for names of retailers. What are some restaurants not in the hotel?

If the person falters, hang up. Use a legitimate telephone number-finding website (I like WhitePages.com, which has a business category) and call that number and ask the same questions. Booking by phone is increasingly uncommon, in part because you may miss legitimate specials, so be sure to ask about Internet rates and then get the real URL.

If all of this has made you queasy, try a travel agent. We have become used to doing it ourselves, but an agent generally isn't going to fall for a fake website. And an agent may be able to get you extra value — a room upgrade or a free breakfast. (That's not too good to be true; that's just good business.)

Finally, trust your intuition. Cope, of the hotel association, said that many people who were taken in by

fake sites thought something was off but ignored that nagging voice in their head. But in this case, pay attention. The price of failing to do so may be much more expensive than a hotel room.

Have a travel dilemma? Write to travel@latimes.com. We regret we cannot answer every inquiry.

Copyright © 2016, Los Angeles Times

This article is related to: Travel, Jack Lew

Published August 2015

How to Spot a Travel Scam

5 things to consider when booking your next vacation

BY STAFF

We've all heard the adage: "If it sounds too good to be true, it probably is." That statement applies to booking travel, too.

While booking travel online offers the ability to compare prices and read online reviews, AAA Travel experts note that scams that target consumers booking travel online have been increasing. The American Hotel and Lodging Association estimates hotel booking scams cost U.S. consumers more than $220 million a year.

When you are researching your next trip online, keep your eye out for ads for super-low pricing on hotels and car rentals, and to-die-for pricing on a cruise or tour. It's possible that the rock-bottom rates are valid, but using a third-party booking site comes with a fair amount of risk. "Some sites look legitimate but aren't," says Amy Moreno, travel manager for AAA Arizona. "These sites, which can resemble legitimate booking travel sites, will take your money but not actually book a room, flight, or car, leaving you without a reservation when you arrive."

Also, if you book through a third-party site and need to cancel or change your trip, you'll likely run into a lot more red tape. Often, the site will refer you to the airline or hotel to request a refund. And if a refund is provided, it might not be for the full amount. Of course, when you use AAA.com (https://www.az.aaa.com/travel/travel-world-aaa) to book your air, car, or hotel rentals, you can travel with the confidence of the largest leisure travel agency in the United States. Plus, if there are any changes to your reservation, AAA Travel can help.

As a trusted travel resource, AAA Travel experts offer these five tips to avoid travel scams and

Learn More

AAA is a go-to source for travel information and can provide security when you book your next trip. Visit AAA.com (https://www.az.aaa.com/travel/travel-world-aaa) or call toll-free 1-888-870-9392.

get the most out of your next trip:

1. Research companies: Book with reputable companies whose names you recognize. Even then, search their name along with "scam" and "review." If you see a lot of negative reviews for a company, proceed with caution. Try looking them up on the Better Business Bureau (http://www.bbb.org/)'s website. Also, ask friends for recommendations of online travel agencies.

2. Use credit cards: Always pay with a credit card and not a debit card. With debit cards, the money immediately is removed from your bank account, which can make getting it back more difficult. It's easier to dispute the charges by using a credit card.

3. Read carefully: Combing through the fine print of travel documents can be tedious, which is why many consumers fail to do this. Even if the site says something like "satisfaction guaranteed," still read the fine print before booking and understand the cancelation and revision policies. This could help prevent inconveniences, such as being charged a higher room rate when you arrive.

4. Verify reservations: For hotels and flights you booked through a third-party site, call the hotel or airline directly to make sure that the reservations are correct and ask the company to notify you of changes. Again, use a credit card to book travel, as it offers you more protection.

5. Use an agent: AAA Travel experts recommend working with a trusted travel agent, especially if you're unfamiliar with the area. Agents are founts of knowledge, keep you informed of changes, and have your back when necessary.

We Also Recommend

How to Fest
(/foodfest)
8 tips to help you get the most out of a food festival
(/foodfest)

5 Cruise Essentials
(/article/5-cruise-essentials)
What to pack for your international voyage
(/article/5-cruise-essentials)

'Twas the Flight Before Christmas
(/article/twas-flight-christmas)
3 tips for simplifying holiday air travel
(/article/twas-flight-christmas)

Servicing AAA members in Arizona
© 2016 Highroads magazine / AAA Arizona

Beware of Online Vacation Scams

Steve Weisman, for USA Today *9:16 a.m. EDT June 27, 2015*

(Photo: dolphfyn, Getty Images/iStockphoto)

Summertime and the living is easy – particularly for scam artists, the only criminals we refer to as artists, who are successfully stealing the money of unwary consumers through phony online hotel booking websites.

According to Maryam Cope, Vice President of the American Hotel & Lodging Association an estimated 2.5 million phony bookings are done each year.

The problem has also gotten the attention of Iowa Senator Chuck Grassley, who has written a letter to the Federal Trade Commission asking them to investigate this scam.

STORY FROM TOURISM AUSTRALIA
Kangaroos and quokkas: Meet Australia's most adorable wildlife
(http://www.usatoday.com/pages/interactives/sponsor-story/tourism-australia-wildlife/)

The scam generally starts when you go online to search for a good deal on a hotel room in a popular vacation spot. Often people will start their search through Google, Bing or other search engines by typing in words such as "discount hotel rooms in Las Vegas."

Merely because a website comes up high in a Google or other search engine search does not mean that the website is legitimate. All it really means is that the scammer is familiar with the algorithms used by Google and the other search engines to rank websites and is able to tailor the website in a manner that will put it high on the first page of a search. No search engine guarantees that the websites that come up high on a search are legitimate.

Sometimes scammers use websites that appear to be those of legitimate hotel chains with which we are all familiar. These websites may carry the logo of the particular hotel and for all intents and purposes appear to be affiliated with the legitimate hotel chain, however, it is a simple matter for a cybercriminal to copy the logo and form of a legitimate hotel's website to make it appear that his phony website is trustworthy.

Merely because the name of a legitimate hotel chain appears in the URL of the website you are using does not mean either that the website is legitimate or has authority to use the hotel's name.

Some of these websites will actually make a reservation for you, however, within the fine print you may find hidden booking fees that make the cost of the hotel room far more expensive than what you would have paid if you had dealt with the hotel directly or had used one of the many totally legitimate discount travel websites, such as Kayak, Expedia, Trivago or Orbitz.

In particular, even if you do manage to book a hotel room through a scammer's online travel website, you may not end up getting the amenities promised, which can be quite important if you require handicap access, for example.

It is important to remember that rarely is there anything fine in fine print and it is important to always read the entire contract before you commit to buy anything. Many people use their smartphones when booking online vacations and the inconvenience and difficulty of reading contract terms on a small smartphone screen can lead to problems.

In a worst case scenario, online travel scammers lure you into providing your credit card number and then don't even make a booking at all, but merely take your personal information including your credit card number and use that information to make you a victim of identity theft.

So how do you protect yourself when booking a hotel room online? Here are some important tips.

1. Trust me, you can't trust anyone. Don't trust websites merely because the name or logo appears to be familiar. You are generally better off limiting your online travel searches to the specific websites of hotel chains in which you are interested or well-established discount travel websites such as Kayak, Expedia, Trivago or Orbitz.

2.Don't trust a toll free number found on the particular website you are using to confirm that the website is accurate. Scammers who set up phony websites also will include phony 800 numbers which, when you call, will be answered by someone who poses as an employee of the legitimate hotel.

3.Read the contract in writing. It may be difficult, particularly if you are using a smartphone with a small screen, but it is critical to understand all of the terms, conditions and costs of your booking before you pay.

4.Use a credit card for your payment because it is much easier to dispute any fraudulent charges and have those charges removed if you use a credit card rather than a debit card.

5.If you do use a discount travel website to make a reservation at a hotel, contact the hotel directly after you have made the reservation to confirm that your reservation has been made and that the details of the reservation are the same as what was promised to you.

6.Never provide personal information or your credit card number online unless the website's URL begins with the letters "https" rather than merely "http." The added letter "s" means that your information is being encrypted and safer to transmit.
7.Finally, your mother was right. If the deal sounds too good to be true it usually is. Remember, trust me, you can't trust anyone.

Read or Share this story: http://usat.ly/1ljMb6T

July 22, 2015, 09:00 am

Close the door on hotel booking scams

By Mary E. Power

I love hotels! One of my fondest childhood memories is accompanying my father, a small town doctor, to medical conferences for his continuing education credits. My brother and I probably drove hotel employees crazy as we explored around, but hotels seemed like such fascinating and exciting places to me. Thanks in large part to these happy memories, I majored in hospitality business management in college and began my career working for two different hotel chains.

Some years later, I find myself at the helm of the Better Business Bureau. Among the many services we provide are Business Reviews that help consumers decide which companies to do business with. We also warn people about bad business practices and illegal scams. Unfortunately, many of those relate to the travel and hospitality industries.

Consumers have come to rely on technology to make their life easier, and that's especially true when coordinating travel arrangements. At **bbb.org**, you can find BBB Business Reviews on more than 60,000 hotels, resorts, motels and other properties. Last year consumers turned to us nearly 400,000 times to check on hotels. Increasingly, online travel booking services have become a key resource for consumers, and we track over 600 of those, as well.

A growing problem is rogue booking sites that mislead and confuse customers trying to make hotel reservations. Online travel bookings are a leading indicator of consumers' confidence in e-commerce transactions – and this scam is eroding that confidence. It's not a small problem. The American Hotel & Lodging Association estimates that 2.5 million bookings a year are misleading. That translates into more than $220 million in bad bookings.

The scariest part of this scam is that it doesn't find you; you find it. Most scammers approach you by email, robocalls or even knocking on your front door. But those who get scammed by rogue booking sites usually began with an online search for their choice hotel. Up pops a link that looks just like the hotel's website. These rogue sites can mirror the design, logos and photos of real companies, and they dupe users into thinking they are doing business directly with the hotel. The URL may include the hotel's name. Some sites even include a "call now" button staffed by call center employees who have a whole script to hide the fact that they aren't actually with the hotel of choice. Far too many consumers end up booking through a third-party site without knowing it.

Deceived consumers often show up at a hotel or resort and find they don't have the right accommodations or they can't get their reward points. Worse, some people show up and find out the hotel doesn't even have a reservation for them!

Even the savviest travelers have fallen for scams like this. These bad players are extremely skilled in the art of deceiving unsuspecting consumers. People who may not be skilled at online transactions, or are more comfortable talking to a "real person," a deceptive call center button may seem like an attractive way to make a booking. Little do these travelers know they aren't talking to the hotel at all.

Smart phones have compounded the problem. Smaller screen sizes mask phony sites, making it more difficult to identify details that aren't quite right, like a phony URL or toll-free number that look like the hotel's direct reservation desk but are really from a third party.

As consumer complaints mount, these practices are not going unnoticed. Recently, the Federal Trade Commission and the Department of Justice have been hearing from Members of Congress and state legislators who want the FTC to open an investigation. Better Business Bureau works closely with the FTC on numerous issues. We send our complaint data into their Consumer Sentinel tracking system; we refer to their consumer education materials; and we assist in investigations. We think the FTC is the right agency to look into these hotel booking scams and rogue websites, and we will do what we can to assist them.

BBB was founded on the truth-in-advertising platform and it's been core to our mission for more than a century. Consumers want and deserve clear, transparent communication when they are transacting online, and the entities that engage in deceptive practices should be held accountable.

No one should have reservations about making reservations online. No one wants headaches and harms when simply trying to book and enjoy a vacation and no one should have to be a detective in order to avoid getting scammed. Check out hotels, booking sites and millions of other businesses at **bbb.org** before you buy.

Power is president and CEO of the Council of Better Business Bureaus, the umbrella organization for 113 BBBs in the United States, Canada and Mexico.

The Hill 1625 K Street, NW Suite 900 Washington DC 20006 | 202-628-8500 tel | 202-628-8503 fax
The contents of this site are ©2016 Capitol Hill Publishing Corp., a subsidiary of News Communications, Inc.

Video Clips Highlighting Booking Scams

Nightline (extended version): http://abcnews.go.com/Nightline/video/pitfalls-booking-hotel-rooms-online-30096646

GMA: http://abcnews.go.com/GMA/video/tips-watch-booking-hotel-rooms-online-30080890

CBS This Morning: http://www.cbsnews.com/videos/travel-scams-found-online-cost-americans-millions/

CNBC clip – conversation on consumer deception:
https://www.dropbox.com/sh/cmngn2tkq84mgmg/AABX8QB0peDH3v6jzHLXPWaCa?dl=0

Yahoo!: https://www.yahoo.com/style/watch-the-online-hotel-booking-scam-thats-117733144787.html