

# Travel scams are getting harder to spot. Here's how to stay safe

By Adriana Morga,  
The Associated Press September 10, 2026



Pickpockets were once the biggest worry for travelers heading to new destinations on vacation.

But travel scams have become more sophisticated, and scammers using new artificial intelligence tools have become better at creating fake websites and using stolen data to their advantage, said Florent Silve, an executive at Engine, a corporate travel management platform.

“What used to look like a fake website now becomes much harder to spot by consumers,” Silve said.

According to a Federal Trade Commission report published in June, Americans last year reported losing \$3.5 billion to scams in which impostors contacted them through text, email, phone, social media and search engines, though those weren't all travel scams. Nearly 1 in 3 fraud reports were about impostor scams, making it the most reported fraud category.

Travel scams can happen before you even hop on a plane, with scammers posing as your hotel or airline to take advantage of the fact that you're expecting to receive communications from those companies.

“In the past, people were like ‘Oh if I receive a scam that is completely out of place, that's how I know it's a scam.’ But now, the most dangerous scams don't look suspicious; they look expected,” said Iskander Sanchez-Rola, a scam expert for Norton, a cybersecurity company.

If you're planning a trip soon, here are some expert recommendations to stay safe from travel scams:

## Beware of reservation hijacking

A new common travel scam is reservation hijacking, Sanchez-Rola said. In this scam, imposters send you an email or text, pretending to be your hotel. They pretend that something went wrong, such as a failed payment, and say you need to take immediate action.

What makes these scams particularly difficult to spot is that scammers often use real information to make you believe they are legit, Sanchez-Rola said. Scammers target hotel systems by phishing hotel staff to get login credentials and then accessing legitimate information from hotels or booking services. Using this information, scammers send you an email with your actual reservation dates or the exact cost of your hotel stay, hoping to convince you they're with the company you used to make the reservation.

“The main thing is that this isn't a fake booking confirmation, it's a real reservation that is weaponized against you,” Sanchez-Rola said.

If you encounter this type of scam, Sanchez-Rola recommends that you don't rush to make a payment through the provided link and instead call your hotel directly. Don't call the number

attached to the email or text you received because it might have come from the scammer. Instead, go to the official hotel website and call the number listed there.

## **Be wary of flight cancellation notifications**

Another popular scam involves flight cancellations, Sanchez-Rola said. Scammers contact you with an urgent message saying your flight has been canceled or delayed, then pretend to help you rebook your flight for an additional cost.

“You’re going to a place, and one day before that happens, they tell you that the flight was canceled,” Sanchez-Rola said. “So in that moment, there is an inherent urgency.”

If you receive a text saying that your flight has been canceled, don’t panic. First, go directly to your airline’s portal and verify the information. If you need to rebook your flight, do so directly with the airline or third-party booking system you originally used. Above all, don’t click on any links sent to you through a text message, Sanchez-Rola said.

To help keep yourself safe from being scammed in the first place, don’t post photos of your plane tickets and other travel documents on social media. Even if you cover your flight number with emojis, the ticket can reveal more than you think.

“The QR codes or the barcodes that are there include a lot of information,” Sanchez-Rola said. “Sometimes they even include information about returning flights.”

## **Beware of QR codes**

In recent years, QR codes have become a popular way to pay your bill at your restaurant table. This may be convenient, but it can also make you a target for scams, said Alissa Abdullah, Mastercard’s deputy chief security officer. Scammers paste a new code overlapping the restaurant’s code and direct customers to a fraudulent payment system.

“You may be sitting at a coffee shop and have a real QR code with a fake one that’s a sticker laid right on top,” Abdullah said.

If you’re suspicious of the payment page or notice a sticker laid on top of another at a restaurant, Abdullah recommends that you speak with a staff member and find a different way to pay, such as cash or a credit card.

## **Be careful when using public Wi-Fi**

It’s very common to connect to a public Wi-Fi network to find your way around a new city or download your plane tickets at the airport. While free Wi-Fi can help during travel, it also carries some cybersecurity risks.

“Sometimes cyber criminals will create a network that looks close to the name of a legit network to dupe you into logging onto their network,” said Brian Cute, chief executive officer and director of the capacity and resilience program at Global Cyber Alliance, a nonprofit focused on reducing cyber risk.

If you access a scammer’s network, they can steal personal information, damage your system, or gain remote access to your devices. If you need to use public Wi-Fi, Cute recommends that you stick to basic searches, like how to get to your hotel, rather than accessing websites such as your bank or email.