How to avoid scammers when you book your next holiday

PLEASE NOTE: This transcription was created using an AI transcription tool and may not be a 100% accurate representation of the recorded audio.

[00:00:09] **James Rowe:** Hello and welcome to Witch Shorts, the podcast that gives you a free taster of one of our magazines every single week. Now on today's episode, I found a piece that was written by Lauren Bell in the September October issue of witch travel, which explores holiday scams and how you can avoid them. With the rise of AI making fakes more realistic, it's more important than ever to know how to recognize a scam from the real deal.

Here's Lauren's peace adapted for the podcast this week. Read by me, James Rowe.

When you think of a travel scam, street con artists or rip off taxi drivers probably come to mind, but you are far more likely to be scammed when booing your holiday and the costs are far higher.

11 million pounds. That's how much UK holiday makers lost to travel scams in 2024. That works out roughly at more than 1,800 pounds per person. Part of the problem is that scammers flood. Our social media feeds with fake deals that are so tempting, they're difficult to ignore. More than half the holiday fraud reported last year, mentioned social media platforms like Facebook, and that number is rising sharply, and it's hardly surprising considering how widespread social media use is now.

In fact, one in five Brits now makes purchases via social media according to YouGov. It's also become easier to create a convincing scam with ever improving AI technology, enabling fraudsters to create sophisticated fake ads and even copy reputable sites in minutes. So with all that in mind, here are six things you can look out for when booking your next holiday.

Number one. Being asked for more money, this scam can play out in different ways. You might receive an official look and email requesting additional payment for your next holiday, often with a vaguely plausible excuse such as a new tourist tax. Never click links in these types of emails. If you do, you'll be taken to a fraudulent website where scammers can steal your credit card details.

Instead, just contact the company directly using a verified number or website to check if you owe anything. But this is unlikely if you paid in full. Another tactic is scammers claiming an earlier flight booking you made isn't confirmed and they need more money because fares have now increased. In this instance, you've already been scammed, so don't pay any more.

There are very few instances where a reputable holiday company or travel agent will ask for more money from you after you've paid already. Ask for your money back and report it immediately to your bank and action fraud. Number two, being asked to reconfirm your details. Common examples of scams like this have targeted booking.com users who receive messages from scammers via booking dot com's messaging service, pretending to be from a hotel or accommodation.

Owner scammers told customers to either reconfirm their card details or pay for their hotels through dodgy links money that they will never see again. They weren't the only ones. Between June, 2023 and September, 2024, action fraud received more than 500 reports of a scam targeting bruen.com users, which resulted in 370,000 pounds in total.

Being lost. bruen.com says It has since introduced new technology to identify suspicious behavior and has tightened security to make it more difficult for hackers, but it could still happen. It can be difficult to tell if messages are genuine or not, so if you're ever unsure, contact the hotel directly outside of the platform to check the message is legitimate.

Number three, receiving an email saying the suspicious activity on your account. Having your social media platforms hacked or your password or payment details stolen is all too common. So it's helpful when companies tell you if your passwords have appeared in a data leak or if you've been hacked. Sadly though, scammers have taken advantage of this too and could send you an email claiming there's been suspicious activity on your account.

As I said already, always ignore a link contained within an email. It could be a phishing scam. If you are ever in doubt, go directly to the website of the company you've been contacted by. Number four, freebies on your holiday. You've just booked your holiday abroad and you're understandably excited. You might even post about it in a Facebook group, discuss it in an online forum, or interact with a post from the holiday provider.

But remember, scammers are always looking to pounce. They can use this as an opportunity to send you a message offering free airport lounge access or a free flight upgrade if they see you've only booked a hotel. Remember, nothing good comes for free. The message offering these freebies will come with a link to claim.

As always, don't click it. It's a scam. Number five, rogue taxi apps. Prebook in a cab via an app is a good way to ensure you won't get taken on the scenic route or be surprised by a steep off meter cost when hailing a taxi at the airport, but it's no longer foolproof. One, which member told us that they used an app to book a taxi in Italy, and both her trips were subsequently canceled by email with a promise that the sizable deposit she had paid would be returned within nine days.

This never happened and she ultimately had to use her credit card provider to reimburse her. If there's an app that doesn't require an upfront payment, such as Uber or Bold Opt for this. And if you don't want to use an app, at least get the name and number of a trustworthy cab frame from your hotel before traveling so you don't end up with an unlicensed cab.

And finally, number six, fake cruise activities. According to the Cruise Mummy blog, this scam usually start in cruise social media, fan groups and forums. A scammer will post about a special event that's taking place during the cruise, such as exclusive wine tasting or private crafting classes. They'll ask for a small fee to reserve your spot or to cover the cost of materials, but when you get there, the event won't exist.

Only ever book onboard activities directly through your cruise line and via a secure payment method. If your cruise company ever emails you ensure it's not a spoof email address by comparing it to previous emails you received from the company like your booken confirmation. If you or a loved one has fallen victim to a scam, the charity victim support offers emotional support to those affected by crimes including fraud.

Visit their website@victimsupport.org.uk.

Thanks for listening to this podcast from Witch, the UK's consumer champion. You can find plenty more advice about what we discuss today in the show notes. There you'll also find a link to become a witch member for 50% off the usual price and offer exclusively available to you are podcast listeners.

Joining, which will not only give you access to all of our product reviews, our app, one-to-one, personalized buying advice, and every issue of which magazine across the air. But you'll also be helping us to make life simpler, fairer, and safer for everyone. Don't forget to hit subscribe wherever you're listening.

That way you'll be notified whenever we release a new episode of which Money, which Shorts or another podcast that we make for you. And if you wanna get in touch with us. Then follow us on social media, where at witch uk, or you can drop us an email to podcasts@witch.co uk. See you next time.