Keep yourself safe from

Advance Booking and Accommodation Verification Scams

Accommodation or advance booking scams happen when you are contacted by fraudsters about an existing booking (this could be for a holiday, a flight or even a stay in a hotel) and asked to complete a payment verification check to prevent your booking being cancelled.

You may receive a phishing email that is designed to replicate a genuine email from the company you have booked with, asking you to click onto a link that directs you to an online payment screen where card details can be entered. Or you may receive a message through your account (this could also be a live chat), where the 'agent' is giving instructions to approve payments within your banking app to complete the payment process.

Victims are often sent a message that is crafted to create a false sense of panic. It could include details for your booking, and make you want to act fast to prevent it being cancelled. These messages could ask you to click on a link and provide your bank or card details. From there, you could be asked to verify the payment or your card details in your banking app or you could be asked if the 'company' can freeze the original booking amount on your card. If you go ahead and verify or agree, this will result in money being taken from your bank account.

Top tips for avoiding advance booking and accommodation verification scams:

- Always check the company's terms and conditions, found on their website, to understand the terms of the booking, along with their payment terms.
- If you receive any unexpected requests to pay for your booking in advance, always contact the hotel, accommodation venue or flight company on a trusted number found on their website. Fraudsters can fake phone numbers to make their calls, emails or text messages seem genuine.
- Check the sender's email address. Be cautious if it looks suspicious or is unfamiliar. Verify the legitimacy by contacting the organisation directly, using the details on their website.
- Be cautious of any emails or messages containing links where you are being asked to complete a payment or provide personal and banking details. Before clicking any links, hover your mouse over them to preview the destination URL if you are viewing the email on a computer. Ensure it matches the official website of the company you've booked with.

If you're ever unsure about a payment you've been asked to make, or already made, get in touch with us on your app or by calling 159. We're here to help you. You might also want to speak to Victim Support, an independent charity that can provide support to victims of crime and traumatic events. Their **helpline** is open 24/7