



## **AIB urges people searching for holidays or flights online to be wary of ‘ghost brokering’ or fake travel companies**

### **Criminals use sponsored ads to defraud people searching for cheap trips**

**31 October 2023**

AIB has issued a warning about a new type of travel fraud that is on the increase internationally known as ‘ghost brokering’. Criminals target people searching for online holiday or flight deals using ads that appear to be legitimate but are not. The ads often appear as ‘sponsored’ and direct customers to fraudulent websites.

The websites appear sophisticated and convincing and often request phone numbers and email addresses to use their search function. Fraudsters then use these details to contact the person via a messaging service such as WhatsApp, to entice them into buying cheap flights or holidays. The person believes the offer is legitimate, pays for the holiday and authorises it. They often receive a booking confirmation from the fake travel company, to create the appearance of legitimacy.

Once the criminal harvests the person’s card and security details, they often make several other genuine holiday bookings with legitimate merchants using the stolen card details, to sell them on to someone else later.

AIB’s Head of Financial Crime, Carol Lawton said “International intelligence shows us that this type of fraud or ‘ghost brokering’ is on the rise and as a result, customers should exercise caution when booking holidays online. These scams are often sophisticated and even use sponsored ads to target people who may assume that the travel company is genuine. Not only does the person lose out on the supposed holiday they booked, they are often further defrauded when the criminals use their stolen card and security details to buy genuine holidays to sell on at a later stage. We ask our customers to always think before they click the link.”

AIB urges people to:

- When making travel bookings online don’t just follow the link. Use the internet to search for the property to ensure it exists and belongs to the person that you are dealing with.
- Check that the person you are dealing with works for the company. Look up the company. Do they have a website? Who owns the company? Are they on well-known travel sites such as Trip Advisor? What are the recommendations like for them?
- You can also ensure any website you use is secure and genuine by checking for the padlock symbol to the left of the web address and *if it’s not there, beware.*
- Check the bank account number you are sending the funds to. Is it in the same country as the property? An Irish bank account has IE in the IBAN, a French one will have FR. It could indicate that there is a problem.
- Make yourself aware of current fraud threats by regularly checking your banks security centre on their website.

**ENDS.**

Contact [louise.y.kelly@aib.ie](mailto:louise.y.kelly@aib.ie), 087 2161545