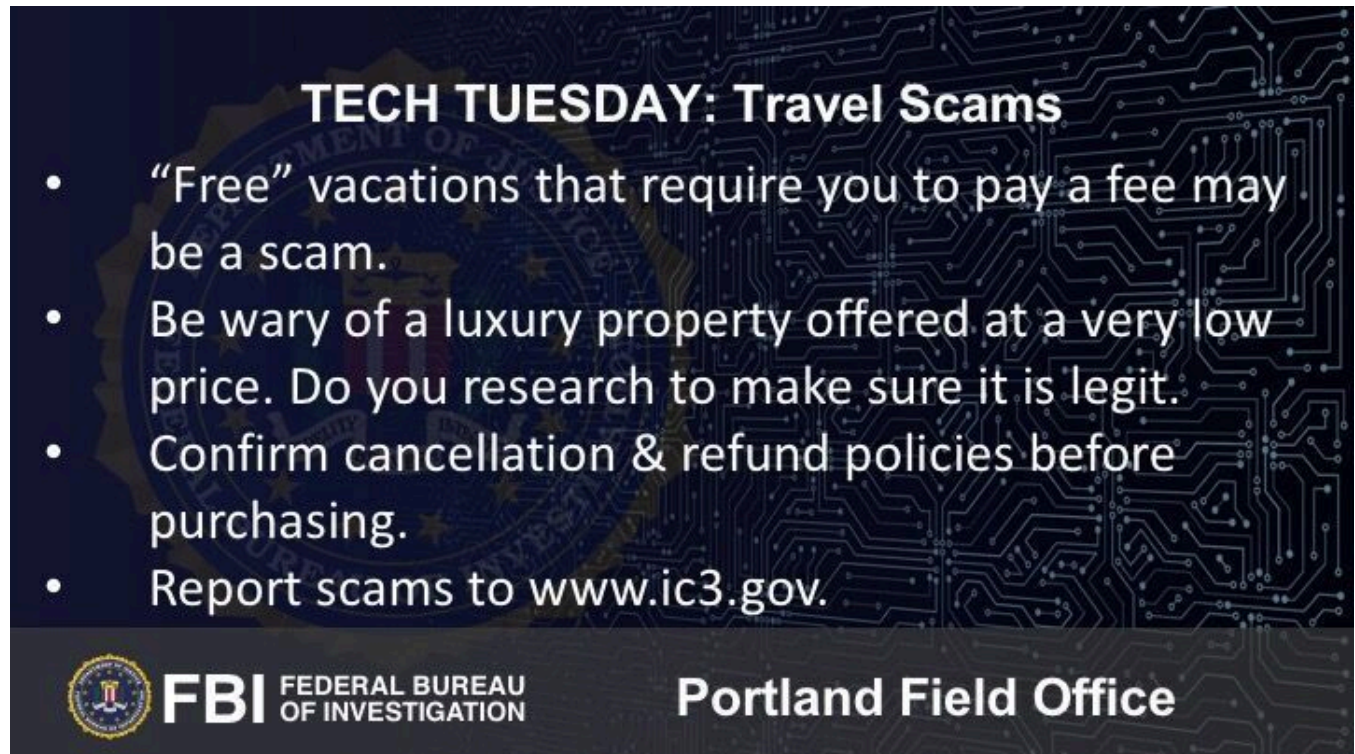


Tech Tuesday: Building a Digital Defense Against Vacation Scams

July 13, 2021

A graphic with a dark blue background featuring a circuit board pattern. On the left is a large, faint circular seal of the Federal Bureau of Investigation. The text is in white. At the top, it says "TECH TUESDAY: Travel Scams". Below that is a bulleted list of four items. At the bottom left is the FBI logo and the text "FBI FEDERAL BUREAU OF INVESTIGATION". At the bottom right is the text "Portland Field Office".

TECH TUESDAY: Travel Scams

- “Free” vacations that require you to pay a fee may be a scam.
- Be wary of a luxury property offered at a very low price. Do your research to make sure it is legit.
- Confirm cancellation & refund policies before purchasing.
- Report scams to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

Welcome to the Oregon FBI’s Tech Tuesday segment. Today: Building a digital defense against travel scams.

It seems as though everyone is desperate to escape this summer... to go anywhere other than your basement office or the neighborhood park. And, finally, with lockdowns lifting, we are getting the chance to travel.

Beware though – scammers are not going to let such a good opportunity go to waste. Your desire to get out drives their desire to cash out at your expense.

Here are some tips from our friends at the Federal Trade Commission (FTC):

Watch out for offers of a “free” vacation that require you to pay fees or taxes to get it.

Pay attention to the details. You get offered a stay at a “five-star” resort or a cruise on a “luxury” ship... but the contact won’t give you more specific details? It’s a red flag if you can’t get the name and address of the hotel or details about the cruise company.

Just say no if the travel offer requires you to pay by wire transfer, gift card, or cryptocurrency. Scammers know that once you pay in one of these ways, it is almost impossible for you to get your money back. Always

pay by credit card.

Don't allow someone to pressure you into making a quick decision about a "great deal." Scammers use social engineering techniques – playing on your fear of missing out – to rush you to act without thinking.

Watch for premium vacation properties advertised for super cheap prices. Below-market rent can be a sign of a scam. Do some extra research to confirm the deal is legit before jumping in.

Get a copy of the cancellation and refund policies before you pay. If you can't get those details, walk away.

Do your own research. Look up travel companies, hotels, rentals, and agents with the words "scam," "review," or "complaint."

Check the address of the property to make sure it really exists. If the property is located in a resort, call the front desk to confirm their location and other details on the contract.

If you are the victim of any online fraud, you should also report the incident to the FBI's Internet Crime Complaint Center at **www.ic3.gov** or call your FBI local office.