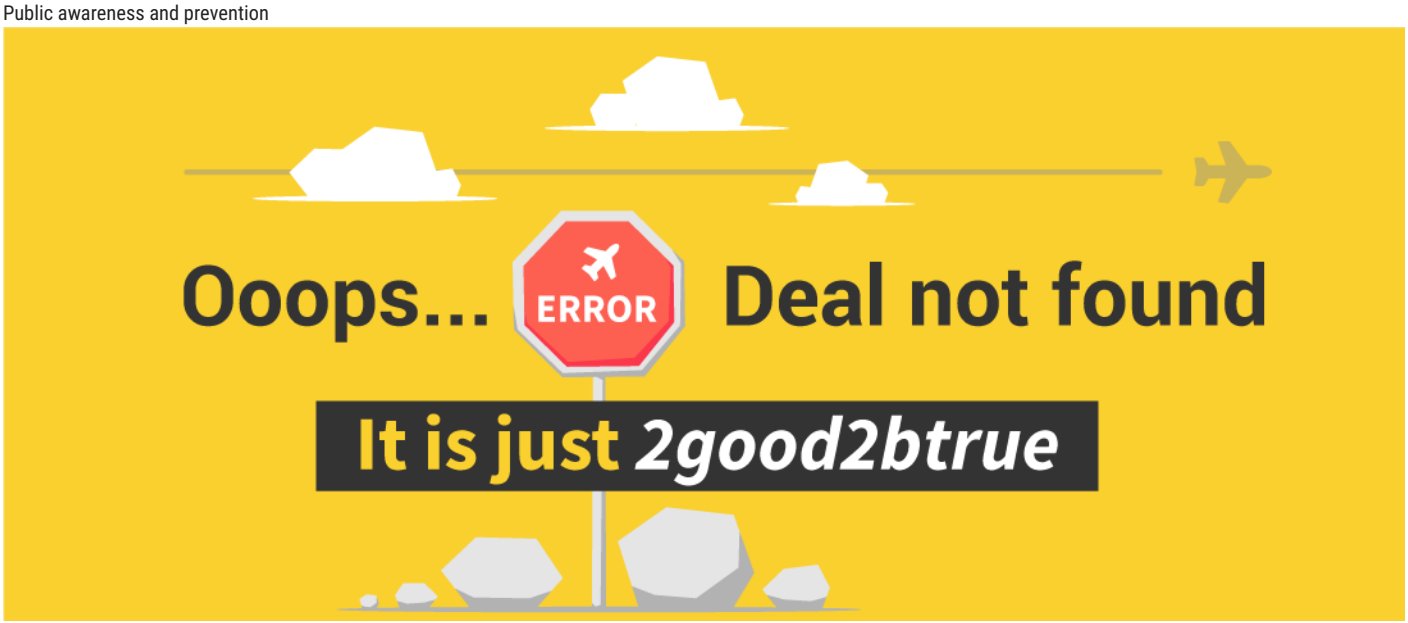
PROTECT YOURSELF FROM HOLIDAY AND TICKET FRAUD

Public awareness and prevention



Sounds too good an offer to be true? That is because it probably is. You've just fallen victim to holiday fraud. From fraudulent flights to non-existing accommodation, holiday fraud is a big business for scammers and is most frequent during peak holiday times, such as summer and December. Holiday makers need to be aware of this. Here are some guidelines if you want to avoid being a victim of holiday fraud.

Everybody enjoys some time off and any moment of the year is time for a well-deserved holiday, whether short haul or long haul. In most cases looking for the dream destination and spotting good deals will be a genuine and problem-free transaction. However, if you book online, you are at risk from fraudsters and potential scams. This page will help you understand the risks and protect your finances and expectations:

IF...

... you find out at the airport that you are not booked on the expected flight;

... once you arrive at your destination the hotel does not have your name booked for a stay;

... the holiday home you booked doesn't exist or the owner is not aware of your reservation;

... the rental car company doesn't have a booking under your name or your request is refused because of a fraudulent purchase;

... the fraudster completely cuts contact after you have paid and will not confirm anything you have booked...

THEN

you are a victim of online holiday fraud. Keep all the evidence and report it to your national police right away.

WHAT IS HOLIDAY FRAUD?

Holiday fraud happens when you pay a travel agent, agency or private entity for rental services offered online such as:

- transport tickets (plane, train, boat, etc.);
- accommodation;
- rental cars;
- complete holiday packages including, all or some of the above;

and find out that the service you booked does not exist or it has been paid not with your money but with a compromised card of another victim, making your purchase invalid.

Often criminals will just be after your money. However, in many cases, scamming you is just part of a grander plan – criminals will use stolen credit card details to buy legitimate travel services, which they then offer to you at a lower price.

1 SNAP UP THAT UNBELIEVABLE DEAL

- **Hotel**
- **Tickets** (plane, train, boat, etc)
- **Car rental**
- **Full vacation package** (including some or all of the above)

2 PAY BEFORE IT'S GONE

We accept

- **Credit / debit card**
- **Bank / money transfer**
- **Virtual currencies**

3 BRACE YOURSELF FOR THE BAD NEWS

Either there is no booking

... or the booking was cancelled

as it was paid with someone else's compromised card

REMEMBER: **If you've paid with your credit/debit card, contact your bank immediately. Otherwise the criminals will be able to use your details in the future.**

WHAT ARE THE WARNING SIGNS?

You are contacted by a travel agent or company you have never spoken to before offering you a holiday at a very low price.

Fraudsters use fake online adverts, bogus sales calls, emails, text messages and instant messaging offering incredibly cheap rates to tempt you into booking a holiday or purchasing a service. If the price is too good to be true, it probably is.

The website looks suspicious

- There are only a few details and pictures of the property or hotel;
- Online reviews aren't favourable or don't exist at all.

You are requested to pay in cash, via bank transfer, such as with MoneyWise or Western Union, or even virtual currencies like Bitcoins.

These payment methods are difficult to trace and are not refundable (remember: criminals need to monetise the stolen card details of other victims and you could be part of this plan).

You are urged to pay quickly

as the fraudster warns you that the property will be let to someone else or the deal will pass unless you commit immediately. The criminals may also claim there is a certain discount for quick payment.

HOW TO PROTECT YOURSELF

ters use fake online adverts, bogus sales calls, emails, text messages and instant messaging offering incredibly cheap rates to tempt you into booking a holiday or purchasing a service. If the s too good to be true, it probably is.

Don't reply to unsolicited emails, texts, instant messaging, social media or calls with holiday offers.

Links and attachments in emails may lead to malicious websites or download viruses on your device.

Book a holiday directly with an airline or hotel, or through a reputable agent/tour operator.

Do a thorough online search to ensure the company is legitimate

- Look for the IATA logo on the company's website;
- Check that the website uses a secure payment system and the secure communication protocol (https) for the booking procedure;
- Check reviews. People may have posted their experiences warning others;
- Pay special attention to the website name and domain. Small changes in the name or domain can direct you to a completely different company;
- Check that the website offers full contact details. A landline phone number, postal address and any other information that would make it easy for you to contact them should anything go wrong;
- Check that the website offers Terms and Conditions, a refund policy and a privacy policy. Make sure they have your consent before sharing any of your data with a third party.

Be wary when buying flight tickets from websites which sell other services, such as cars and holiday homes.

You can check if the flight exists by consulting the airline's own website.

Dealing directly with the property owner or a private agent? Stay alert!

- Request additional pictures and ask them questions about the booking, room, WI-FI connection, location and area;

- Don't book on websites that don't have a padlock icon (https) in the address bar;
- Be extra cautious if you are asked to pay using bank transfer or cash; always pay by credit card so your purchase is protected, or use a secure payment site such as PayPal.

After the purchase,

- check that you have received the necessary e-tickets or booking documents;
- review your personal information, dates, hotel details and flight numbers and times;
- try to confirm directly with the airline, car rental or hotel that the reservation is done.

IF...

... you pay for the tickets, but they are not delivered;
... you call the company you bought the tickets from, but your calls are not answered or you are told the company does not provide refunds;
... you are told that a customer representative will meet you at the venue on the day to give you your ticket, but nobody shows up;
... you receive the tickets by post or email as e-tickets, but when you arrive at the event, your entrance is denied by security because the ticket is fake or stolen.

THEN

you are a victim of online ticket fraud. Keep all the evidence and report it to your national police right away.

WHAT IS TICKET FRAUD?

Ticket fraud happens when you buy tickets online from a website or agent for any event that requires a ticket for admission, whether a music concert or festival, a sporting event, such as a football match, or a live show performance, but the tickets either do not arrive or turn out to be fake or stolen.

WHAT ARE THE WARNING SIGNS?

The tickets advertised are either already sold out on the website of the official sellers, or have not officially gone on sale yet, but you find a website claiming to have tickets available.

In some instances, the event promoted does not even exist.

The website address is very similar to a legitimate ticket sales website.

Fraudsters create their own bogus ticket retail companies; their websites are easy to make and look genuine. However, giveaways include a web address that starts with http (instead of https) and the absence of the locked padlock within the address bar.

The website is advertised via email or social media offering you the chance to buy tickets to a popular event.

This could be a form of phishing; fraudsters take advantage of the huge demand for the most popular events.

Limited contact details displayed on the site you are buying the tickets from.

There should be a landline phone number and a full postal address.

HOW TO PROTECT YOURSELF?

Think twice before clicking on any emails, instant messaging or social media that claim to be offering tickets, as they could direct you to a fraudulent site or infect your device with malware.

Only buy tickets from the venue's box office, the promoter, an official agent or a well-known and reputable ticket exchange site. Promoters normally inform you of other legitimate points of sale. Always contact them in person or check on the internet that you are dealing with an authorised seller.

Check the seller's return policy and always keep the receipt until after the event.

Do your research to ensure the company is legitimate:

- Check that the website uses a secure payment system and the secure communication protocol (https);
- Check the reviews. People may have posted their experiences warning others off. Or there might not be reviews at all;
- Pay special attention to the website name and domain. Small changes in the name or domain can direct you to a completely different company;
- Check that the website has full contact details. A landline phone number, postal address and any other information that would make it easy for you to contact them should anything go wrong. If the site does have a 'Contact us' page but only offers a form to fill out, this can be an indicator of a fraudulent website;
- Check that the website offers Terms and Conditions, a refund policy and a privacy policy. Make sure they have your consent before sharing any of your

data with a third party.

If you are buying football tickets, bear in mind that it's illegal for anyone to re-sell them in most instances.

Pay for your tickets by credit card if you can. This will offer increased protection over other payments methods, such as debit card, cash, or money transfer services.

If you choose to buy tickets from an individual, never transfer the money directly into their bank account, but use a secure payment site such as PayPal.

Apply common sense when finding tickets available for an event that has already officially sold out, or that hasn't officially gone on sale yet.

CRIME AREAS	Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES	European Cybercrime Center (EC3)
