

## Hajj fraud warning issued by Civil Aviation Authority over fake Makkah deals.

The Civil Aviation Authority's campaign is working to protect travellers after an increasing trend in the sale of illegal or fake package deals. In the worst cases, these illegal vendors have been prosecuted and imprisoned.

With over 25,000 British Muslims expected to make the Hajj pilgrimage this August, the Civil Aviation Authority is launching a campaign to ensure that this often once in a lifetime trip is not scuppered by booking through a disreputable company, or those falsely posing as reputable travel agents.



### Always follow Action Frauds top five Hajj travel tips:

1. **Check for ATOL protection:** Look for the ATOL logo on your travel company's website, brochure or shop front.
2. **Research your trip:** Some companies will incorrectly claim to have ATOL protection. Check the company's name on the online database at: [www.packpeaceofmind.co.uk](http://www.packpeaceofmind.co.uk).
3. **Check if your package includes a visa:** Appoint a licensed travel agent and ensure that they are arranging a visa as part of your arrangements.
4. **Watch out for hidden costs:** Make sure you check the airport and accommodation fees, such as baggage allowance and accommodation transfers, to avoid any surprises.
5. **Check financial protection if booking with non-UK travel companies:** There are some non-UK travel companies which offer Hajj travel to UK consumers, but these will often not be ATOL protected. Do your research and check what financial protection they provide. Visit [www.packpeaceofmind.co.uk](http://www.packpeaceofmind.co.uk) for more information about ATOL protection.

### If You Are Affected

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or <http://www.actionfraud.police.uk>

If you would like support as a result of becoming a victim of any crime, contact [Victim Support](http://www.victimsupport.org.uk) on 01926 682 693.

## Fraudsters Send Fake Virgin Media Emails Threatening "Automatic Disconnection"

Action Fraud has received over 100 reports about fake emails that purport to be from Virgin Media. The emails threaten the recipient with "automatic disconnection" due to "invalid billing information". The links in the emails lead to genuine-looking phishing websites that are designed to steal your Virgin Media account login details.



### Top Tips:

- Don't click on the links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details.

## ABTA Website: Holidaymakers Hit By Cyber Attack

About 1,000 files accessed may include personal identity information of individuals who have made a complaint about an Abta-registered travel agent. It says it is contacting those affected by the hack which happened on 27 February and has a dedicated helpline. It has also alerted the police and the Information Commissioner's Office (ICO), as part of the ICO's role is to help the public manage their personal data.

### It said the type of data which may have been accessed included:

- Email addresses and encrypted passwords of Abta customers and members registered on the website
- Contact details of customers of Abta members who have used the website to register a complaint
- Data uploaded to support a complaint made about an Abta member since 11 January 2017
- Data uploaded by Abta members in support of their membership

### Top Tips:

- If you are a member registered on the ABTA site, it is advised that you change your password as a precautionary measure.
- If you have uploaded contact details or documentation on the website, you should actively monitor their bank accounts, social media and email accounts, and remain vigilant.

### If You Are Affected

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or <http://www.actionfraud.police.uk>

If you would like support as a result of becoming a victim of any crime, contact [Victim Support](#) on 01926 682 693.

### MONTHS TOP TIPS:

#### MONTHS TOP TIP:

#### Book Your Holiday's Safely:

- Always use websites which have a green padlock and HTTPS within the address bar when paying for a holiday online.
- Verify a company is genuine by checking their ABTA/ATOL numbers on the ABTA or ATOL websites.
- When you are on holiday – DON'T post on social media that you are away (you might be letting potential criminals know your house is empty).

### Keep up to date with the latest updates on Community Safety in Warwickshire.

Like us on **Facebook:**

[www.facebook.com/SafeinWarwickshire](http://www.facebook.com/SafeinWarwickshire)



Follow us on **Twitter:** [@SafeInWarks](https://twitter.com/SafeInWarks)



Visit our **site:** [www.safeinwarwickshire.com](http://www.safeinwarwickshire.com)

## TV Licensing scam that has cost victims over £830,000 and how to spot it.

An ongoing TV Licensing phishing campaign, first identified by the National Fraud Intelligence Bureau (NFIB) in September 2018, continues to be reported to Action Fraud in high numbers. Fraudsters are sending members of the public fake TV Licensing emails that are designed to steal their personal and financial information. Since April 2018, Action Fraud has received over 900 crime reports with victim losses totalling more than £830,000.



### How you can protect yourself:

Don't click on the links or attachments in suspicious emails and never respond to messages that ask for your personal or financial details.

Don't assume a phone call or email is authentic, even if someone knows your basis details (such as your name or address). Remember, criminals can spoof phone numbers and email addresses to appear as companies you know and trust, such as TV Licensing.

Your bank will never call and ask you for your PIN, full banking password, or ask you to transfer money out of your account.