**Subject: Cybercriminals defrauding citizens going on holiday as travel restrictions ease.**

## Threat Summary

Fraudsters always take advantage of disasters, manmade or natural. They use multiple avenues to steal money from unsuspecting citizens, including frauds related to travel. After long period of lockdown due to the coronavirus pandemic, people are more eager to go on a holiday and relax with family and friends. A new trend of using travel advertisements, by impersonating travel agency personnel and creating fake travel websites, for defrauding citizens has been noticed.

## Modus Operandi

- Fraudsters approach victims through an advertisement, Fake travel website or social media platforms**.**
- Names of online booking platforms, such as MakeMyTrip, Airbnb, etc., are generally misused in such ads, websites and social media pages.
- Many citizens have fallen victim to such frauds in below mentioned ways;


*Fig. 01 – Sample image showing advertisement by fraudsters for travelling*

i. Fake advertisements: Cybercriminals get hold of the victims when they respond to fake travel advertisements circulated on social media. Then the victims are convinced by fraudsters to transfer money for buying fake travel packages.

ii. Impersonating travel agents: Fraudsters randomly contact victims purporting to be from a travel company or an airline to offers incredible discounts on travel packages. Victims are taken through the booking procedure and the take payment is taken via online banking methods.

iii. Fake travel websites: Fraudsters create fake travel websites and fake holiday accommodation websites to lead victims to make bookings.

- Victims fall prey to these ways used by cybercriminals and lose their hard-earned money by booking such travel packages, flight tickets, accommodation packages, etc.
- Victims become aware that they have been defrauded when the contact is discontinued by fraudsters and they lose booking amount.

**Suggestions:**

- Thoroughly scrutinize any unknown person offering a great travel deal on the phone or through social media/email.
- Check such website URLs for legitimacy, and if altered by slight changes to domain names.
- Thoroughly search online the travel company, and the package provided, to ensure credibility of the company.
- Always remember, if a deal sounds too good to be true, it probably is.
- Report any such incidents on the ***cybercrime.gov.in*** portal and follow ***@CyberDost*** on Twitter to know more about safety tips.

Regards

Threat Analytics Unit (TAU)
**Indian Cyber Crime Coordination Centre**
CIS Division, MHA
011-23438207