Research Report on

CYBERCRIMINALS LURE INTERNET USERS TO GET INTO A FREE FLIGHT TRIP SCAM

WITH THE NAME OF EMIRATES AIRLINE
This report is purely based on technical findings made by the research team during an investigation. It does not intend to malign or in any way target any country, actor or person. All the information provided in this report has been extracted during the investigation and information might be changed after generating the reports.
RESEARCH REPORT ON

CYBERCRIMINALS LURE INTERNET USERS TO GET INTO A FREE FLIGHT TRIP SCAM WITH THE NAME OF EMIRATES AIRLINE

The Research Wing of CyberPeace Foundation received a message over Whatsapp containing a suspicious link that lures users with a vacation giveaway pretending to be an offer from Emirates Airline.

Link

https://tinyurl5[.]ru/r574461147/

Summary

⚠️ WARNING SIGNS ⚠️

- The campaign is pretended to be an offer from Emirates Airline but is hosted on the third-party domain instead of the official Emirates Airline website which makes it more suspicious.
- The domain names associated with the campaign have been registered in very recent times.
- Multiple redirections have been noticed between the links.
- No reputed site would ask its users to share the campaign on WhatsApp.
- The prize is kept really attractive to lure the laymen.
- Grammatical mistakes have been noticed.

☀️ CYBERPEACE ADVISORY ☀️

- CyberPeace Foundation recommends that people should avoid opening such messages sent via social platforms.
- Falling into this trap could lead to whole system compromise such as access to the microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications, etc as well as the financial loss for the users.
- Do not share confidential details like login credentials, and banking information with such a type of scam.
- Never share or forward fake messages containing links to any social platform without proper verification.
- There is a need for International Cyber Cooperation between countries to bust the criminal gangs running fraud campaigns affecting individuals and organisations to make Cyberspace resilient and peaceful.
Case Study

The Research Wing of CyberPeace Foundation along with Autobot Infosec Private Limited has looked into this matter to reach a conclusion that the website is either legitimate or online fraud.

On Visiting the link users were redirected to

https://tinyurl5[.]ru/r574461147/#XX

**Where XX represents a unique 13 digits number, for example 166166167260.**

On the landing page, there is an image of Emirates Airline and a message that says - (Hello, This is Emirates Vacation Giveaway - hurry up opportunities are melting away !.)

At the bottom of this page, there is a section that seems like a social-media comment section.
The user has to answer four questions, answer this short quiz, find the golden ticket and win up to 2 round-trip tickets to Europe, Asia or Domestic flights. 72 tickets left. Questions are like

“Do you know Emirates Airline?

How old are you?

How do you think of Emirates Airline?

Are you male or female?” etc.

After answering all four questions a congratulatory message appears.

“Congratulations!
Your answer has been saved successfully! This is your chance! You must select the correct box with your prize inside. You have 3 attempts. Good luck!”

After clicking the OK button users are given three attempts to win the prizes with multiple gift boxes.
On the 2nd attempt, it says that the user has won a (2) round trip tickets to Europe, Asia or Domestic Flights with an attractive image of Boarding pass.

“Congratulations!

You did it! You won the (2) round trip tickets to Europe, Asia or Domestic flights.

1. You must tell 5 groups or 30 friends about this promotion.

2. Enter your delivery address and complete the registration”

Clicking on the ‘OK’ button, it instructs users to share the campaign on WhatsApp, strangely enough, the user has to click the WhatsApp button until the blue bar reaches 100%.
After clicking the Continue button, a new box appears, here the user has to complete registration according to the given steps.

**Congratulations!**

Your prize is: (2) round-trip tickets to Europe, Asia or Domestic flights. Follow the instructions below to receive it at your home!

**Congratulations! The last step:**

1. Before we can send your gift, you must fill out the form by clicking on "FINISH"
   (Remember that this step is very important)

After completing the above instructions, wait for the administrator to check, the review will be completed within 24 hours.

**FINISH**

When the user clicks on the Complete registration button it redirects users to multiple advertisement pages and it varies every time the user visits the URL.
IN DEPTH INVESTIGATION:

Some of the key findings are as follows:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>tinyurl5[.]ru</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [OK]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.195.165</td>
</tr>
<tr>
<td>ISP</td>
<td>CloudFlare Inc.</td>
</tr>
<tr>
<td>ASN</td>
<td>13335</td>
</tr>
<tr>
<td>Country</td>
<td>United States</td>
</tr>
</tbody>
</table>

Domain: TINYURL5.RU  
State: REGISTERED, DELEGATED, VERIFIED  
Person: Private Person  
Registrar: R01-RU  
Admin-contact: https://partner.r01.ru/contact_admin.khtml

Created: 2022-04-06T03:48:29Z  
Paid-till: 2023-04-06T03:48:29Z  
Free-date: 2023-05-07

Source: TCI
In source code analysis we found some information like –

- The title of the page is “Emirates Airlines 2022 Vacation Giveaway”

We found three Google tag manager IDs (G-9X98Y9K1R3) in the source code.

The section which seems to be a social media comment area is static and not a dynamic one. The section has been created with some HTML and CSS.
Users are insisted on sharing the campaign with WhatsApp friends and groups.

With the purpose of pushing the notification and tracking the user, Onesignal SDK has been used.
CONCLUSIVE SUMMARY:

The campaign is pretended to be an offer from Emirates but hosted on the third-party domain instead of the official website of Emirates Airlines which makes it more suspicious.

During the investigation we have noticed multiple redirections between the links.

We have investigated the URLs in a secured sandbox environment where the WhatsApp application was not installed. If any user opens the link from a device like a smartphone where the WhatsApp application is installed, the sharing features on the site will open the Whatsapp application on the device to share the link.

The prizes are kept really attractive to lure the laymen.

The domain name associated with the campaign has been registered in very recent time.

Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front-end domain names used in this campaign.
CyberPeace Advisory:

CyberPeace Foundation and Autobot Infosec recommend that people should avoid opening such messages sent via social platforms.

If at all, the user gets into this trap, it could lead to a whole system compromise such as access to the microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications, etc as well as financial losses.

Do not share confidential details like login credentials, or banking information with such a type of scam.

Do not share or forward fake messages containing links without proper Verification.

There is a need for International Cyber Cooperation between countries to bust the cybercriminal gangs running the fraud campaigns affecting individuals and organizations, to make Cyberspace resilient and peaceful.

Issued by:
Research Wing, CyberPeace Foundation.
Research Wing, Autobot Infosec Private Limited.