Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 152 **14-06-2022**

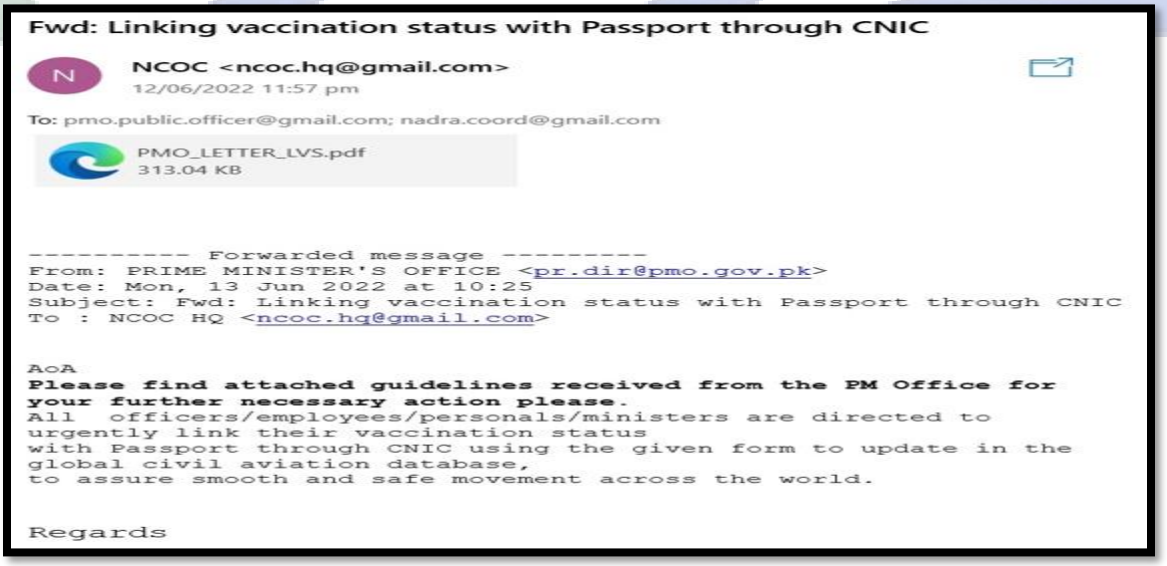
Name: Phishing Email

Threat Classification: Phishing Email from unknown source containing a malicious attachment

Summary:

Email phishing refers to the act of creating and sending fraudulent or spoofed emails with the goal of obtaining sensitive financial and personal information. It can also be done by sending a malicious attachment or link from unauthorized or unknown domain to obtain target data.

A targeted phishing email is circulating with Subject **"Linking vaccination status with Passport through CNIC"** through sender **ncoc.hq@gmail.com** and **pr.dir@pmo.gov.pk**. Phishing email has malicious attachment "**PMO_LETTER_LVS.pdf**". A sample of such email is given below:



Fwd: Linking vaccination status with Passport through CNIC

NCOC <ncoc.hq@gmail.com>
12/06/2022 11:57 pm

To: pmo.public.officer@gmail.com; nadra.coord@gmail.com

PMO_LETTER_LVS.pdf
313.04 KB

---------- Forwarded message ----------
From: PRIME MINISTER'S OFFICE <pr.dir@pmo.gov.pk>
Date: Mon, 13 Jun 2022 at 10:25
Subject: Fwd: Linking vaccination status with Passport through CNIC
To : NCOC HQ <ncoc.hq@gmail.com>

AoA
Please find attached guidelines received from the PM Office for your further necessary action please.
All officers/employees/personals/ministers are directed to urgently link their vaccination status with Passport through CNIC using the given form to update in the global civil aviation database, to assure smooth and safe movement across the world.

Regards

Severity	**High**
Attack Vector	**Phishing**
Privileges required	**None**

Recommendations:

- It is strongly advised to stay vigilant and to avoid clicking on links, or opening attachments in emails from unknown sources. Such emails should be immediately reported to PTA Telecom CERT Portal.
- It is recommended to use secure email gateway to detect the phishing links and malicious attachments.
- Use Potential malicious file types (macro-office files, exe, etc.) must be blocked at the network level on an immediate basis
- DMARC, DKIM and SPF to be implemented across email infrastructure.
- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.