Subject: **Prevention Against Cyber Scam - Nadraonline.com (Advisory No. 9)**

1. **Context.** Recently, it has been reported that overseas Pakistani's are being targeted by online cyber campaign (https://www.nadraonline.com), that lures the individual into filling a user friendly NADRA form and claims to deliver citizen documents like CNIC, POC (Modification of CNIC) and FRC (Family Registration certificate). the website also charges a fee of 65 dollars for home issuance of documents, due to which many citizen are complaining that they haven't received their documents, even after submission of document and fees.

2. **Summary of Cyber Scam.**

   a. **Type of Attack.** Personal Data Stealing and Financial Cyber Scam

   b. **Website Main Features.**

      (i) Website has valid digital certificate

      (ii) It masquerades as valid NADRA website with nearly similar forms.

      (iii) It is inaccessible in Pakistan implying that their intention is to target overseas citizens as well as to remain off the grid from Pakistan cyber space to avoid blacklisting.

      (iv) Website is operational since 2 years and its whois information is as following:-

      (a) **Domain Name.** nadraonline.com

      (b) **Registrar WHOIS Server.** whois.godaddy.com

      (c) **Registrar URL.** http://www.godaddy.com

      (d) **Updated Date.** 2020-05-04

      (e) **Creation Date.** 2018-05-08

      (f) **Registrar.** GoDaddy.com,LLC

      (g) **IP Address.** 162.241.85.70

      (h) **Admin Name:** Registration Private

      (i) **Admin Organization:** Domains By Proxy, LLC

3. **Recommendations**

   a. Presence of https doesn't necessarily means that website is official or authentic. All government / official websites of Pakistan use **gov.pk** or first letter of province in their domain like gos.pk (Government of Sindh) or **gop.pk** (Government of Punjab).

   b. Always double check domain / website information before online payment as most of the time money transferred through services like Western Union, Money Pak, Money Gram etc is nearly impossible to recover in case of fraud.

c. Don't submit private information on unofficial / insecure websites for registration of accounts as that can be used for online harassment, blackmail, hacking or identity theft.

d. Keep credit / debit card information including banking account passwords private.

e. It is mandatory to utilize 2-factor authentication on all social media, email and banking accounts to safeguard against malware and social engineering attacks.

f. Never forward OTP (one time password) received on phone or email to anyone.