Subject: **Advisory - Social Engineering - Vishing Calls related to Covid-19 Vaccination (Advisory No. 35)**

Background. **Social Engineering** is the most successful technique that can effectively lead to sensitive information compromise / stealing and launching cyber-attacks. Phishing over the phone **(Vishing)** is one of the commonly used Social Engineering tactic. Recently, news is circulating on Social Media regarding mobile phone hacking through **Covid-19 Vaccination call.** Further investigation revealed that the news is a hoax, however, Vishing calls can be used by Cyber threat actors to trigger cyber-attacks or gain sensitive information like OTP **(One Time Password), banking information** and Personally Identifiable Information **(PII).** Therefore, recommendations/ preventive measures at **Para 2** must be adopted to avoid becoming victim.

2. **Recommendations**

a. **Official Calls related to Covid-19.** Government of Pakistan / National Command & Operation Centre **(NCOC)** only uses **Help Line Number 1166** related to Covid-19 vaccination and other guidelines. Covid-19 related **calls other than 1166 must be avoided.**

b. **Launching Complaint to PTA against Vishing Calls.** To block spamming / unsolicited communication, type spammer's cell number and followed by space paste the received message; and send this **SMS at 9000.** In addition, following techniques may also be used: -

(1) Vishing call / sms blocking facility is available by calling 420 or by dialing *420#.

(2) Launch online Complaint at **complaint@ pta.gov.pk.**

(3) Toll Free Number **080055055** & Fixed Line Number **0519225325** may be used for launching complaint.

(4) Complaint can also be submitted by Post Mail at the address: -

CPD, PTA HQ Sector F-5/1, Islamabad. In-person visit at this address may also be paid to report the complaint.

c. **General Preventive Measures**

(1) **Mobile Phone Calls**

(a) Vishing calls having country code other than Pakistan (+92) Must be immediately disconnected.

(b) All under command be sensitized not to share personal information, passwords or sensitive information on phone calls.

(c) To counter social engineering phone call, always ask relevant questions from caller and carefully judge him/ her to ensure authenticity.

(2) **Email / Social Media / Other Apps**

(d) Do not **forward**, **click** or **view link** or **photo** sent on email / WhatsApp received from unknown sources / nurnbers.

(e) One-Time Password (**OTP) must never be shared with any one** as it can compromise two-factor authentication.

(f) **It is mandatory to apply 2x factor authentication** on all email, social media and banking accounts.

(g) Do not install untrusted software / applications from **third party sources** on Windows and Android phone.

(h) Do not install unnecessary plugins on browsers except Adblock and Adblock plus.

(i) Always install and regularly update well reputed antimalware solution on both Windows / Android phones.

* * * * *