Subject: **Advisory – Phishing Emails Targeting Top Ranked Civil and Military Officials (Advisory No. 22)**

1. **Introduction.** An email server is a vital part of any IT infrastructure and it is difficult to operate without operational email. However, lack of security practices like encryption, antispam and anti-phishing mechanism, email server may fall prey to hostile elements attempts. Many mail servers operating within sensitive organizations of Pakistan (well reputed government and defense organizations) are observed to be less secure and are under continuous threat of HIA monitoring and interception. Therefore, it is strongly recommended to follow secure email practices to prevent against nation state intrusions.

2. **Recommendations for Email Server Administrators.**

Following recommendations must be followed in true spirit for prevention against hostile espionage and threat actors: -

a. For secure communication, **email server should be hosted on secure domains with valid / verified HTTPs SSL certificate.** SSL certificate can be obtained from trusted vendors like GoDaddy, GlobalSign or Verisign etc, moreover, free SSL certificates may also be obtained via certificate authorities like LetsEncrypt (letsencrypt.org) or ZeroSSL etc.

b. **To combat against Spamming, Spoofing and Phishing,** enable **SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting and Conformance)** in DNS record.

c. Always verify and test the domain for above configuration **by checking via online websites like dmarcian.com (DMARC Inspector), dkimvalidator.com (DKIM Validator) and mail-tester.com (Spam Test). If email server doesn't qualifies the test then it shouldn't be deployed in production environment.**

d. It is mandatory **to turn on STARTTLS on email servers** and **test it** after deployment and configuration via **https://www.checktls.com/Test Receiver (Online TLS Checker).** If any of the **test fails then email server shouldn't be deployment in production environment**

3. **Recommendations.**

a. All email attachments sent must be encrypted with password and password must be communicated through SMS, Call or WhatsApp message.
b. Always confirm the identity of the individual to whom email is being sent or received.
c. Never open attachments from untrusted sources.
d. Endpoint on which official email is being accessed / sent should be secured via well reputed, licensed and updated antivirus solution. Never forward your OTP (One time password) to anyone.