Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 29)**

1. **Introduction.** It has been reported that suspicious activities have been carried out from email IDs of government officials. Attackers hack the email server/ account of individuals and use it for malicious purposes.

2. **Implication of Hacked email account/ Server.** These compromised emails accounts have serious implications as under:-

a. Compromised email account can be used for sending malwares to other sensitive users.

b. Compromised email account can be used for social engineering of senior government officials.

c. These accounts can be used for spreading misinformation as recipient will trust the information being accurate as originated from official email IDs.

d. These accounts can be used by non-state actors for carrying out terrorist related activities while remaining anonymous.

3. **Mitigation Measures.** Following mitigation measures are suggest to limit the attack surface:-

a. **Security of Email Server**

(1) Enable **SMTP** authentication to control user's access.

(2) **DKIM, SPF** and **DMARK** record should be enabled.

(3) Enable TLS (enforcement) for secure email communication.

(4) To ensure security always follow the rule; **no default settings.**

(5) Disable open Relay.

(6) Admin panel should only be accessible via VPN / specific IP.

(7) Activate Reverse DNS to block bogus sender.

(8) Enable **two factor authentication** for accessing webmail.

(9) Use DNSBL server to fight incoming email abuse.

(10) Limit connections to protect your server against DoS attack.

(11) Enable per hour email sending limit.

(12) Deploy security mechanism against **brute force** and **DDoS attack.**

(13) Don't forget to apply updates whenever released by vendor.

(14) Delete the accounts of Ex- Employees / unused email accounts.

(15) Always use strong password (uppercase, lowercase, special character) and disable root access.

(16) Regularly monitor logs of email server for any suspicious activity.

b. **Security of Email Account**

(1) Always use strong and unique password and don't write the password at anywhere.

(2) Never select **yes** to **"Remember password"** in web browser/ email client.

(3) Change password in periodic fashion at least after every month.

(4) Don't open email on Public Internet café or airport.

(5) Install updated and well reputed anti-virus like semantic, Kaspersky etc.

(6) Use two factor authentication for accessing emails.

(7) Don't use one account for multiple purpose.

(8) Don't open email from unknown sender.

(9) Don't download email attachment unless sure about the source.

(10) Don't use official email for private/ personal messages.

(11) Scan all emails for viruses and malwares before opening.

(12) Never access emails from public WIFI.

(13) Never click the "unsubscribe" link in spam emails.

(14) Don't share password with anyone in official staff, always check email in person.

(15) Don't share password during phone call or text message.

(16) Block email with many recipients.

(17) Add legal footer, make sure that each email that is send out includes the necessary legal footer.

4. **Recommendations**

a. Regularly check the vendor website for updates and release of **security patches** of all operating systems/ softwares deployed.

b. Strictly follow mitigation measures discussed at Para 3a&b.

c. Carryout **Penetration testing** and vulnerability assessment of **email servers** for security strength of servers and services.

d. Shared hosting of email server is strictly not recommended. **Approach service provider** for confirmation of hosting details.

e. Train employees on email security to acquire basic awareness of cyber security.

,