Subject:- **Advisory - Prevention Against Cyber Espionage (Advisory No 16 September 2016)**

1. Recently several emails and SMS (being sent to officers and staff of Government departments) have been reported and evaluated that show a **new trend** in **phishing attacks using email and SMS for stealing username/password of targeted users**.

2. **Phishing Emails**

Ser	Subject	Email Sender Impersonating Official Address
a.	Gmail linked to New Mobile Number	alertsystemmailer@gmail.com
b.	Account verification for Gmail	thaiwashin@hotmail.com
c.	Security Measures for Gmail	Service.secure.verify@gmail.com

3. **Phishing SMS**. Various users have received **fake SMS from Gmail** asking them to **change security setting**. SMS are received from random Pakistani and foreign numbers.

4. **Recommendations**.

a. Install and updated well reputed antiviruses such as Kaspersky, Bitdefender, Nod 32, Avast etc.

b. Avoid checking spoofed emails and mark them as spam.

c. If you have clicked on the link then immediately change passwords of email accounts.

d. Use and update **Chrome** of **FireFox** and install "Web of Trust" plugin to view rating of page before opening it.

e. Enable "Two Factor Authentication" in all email accounts.

f. Never open links received in SMS from unknown and known contacts.