Subject:- **Prevention Against Phishing Email (Advisory No. 02,) February, 2015**

It is intimated that various spear-phishing emails are being received by users of government and sensitive organizations. Subject emails contain various types of malware / exploits which are aimed at stealing sensitive information and taking full control of computers.

2. **Detailed Analysis of Email.** Original email received is attached at Annex A. Detail findings are is under:-

a. E.mail Originator. google.update.notification@g.mail.com

b. Subject of Email. "Unusual activity on your mail account"

c. The Email warns user about unusual activity on email account and asks to update IP address and offers some new security update

d. Clicking the link "Update Here" opens a fake gmail login page hosted at "http:// mails goooglenotification.esy.es/" (Annex-B)

3. **Comments.**

a. Phishing site is recognized by at least four security vendors as Malicious.

b. This phishing email is meant for collection of usernames & passwords of targets. Hostile quarters may use the information for further intelligence/information gathering operations.

4. **Actions Taken.** Malicious link has been blocked at National Gateways.

5. **Recommendations.** In order to prevent the leakage of sensitive/personal information, following is suggested:-

a. Avoid opening email from unknown sources specially having official subject matter.

b. Before clicking a link in any internet browser, hover mouse on the link and view actual URL in status bar (bottom left).

c. Before entering login/passwords of email or social networking WebPages, ensure that actual webpage is open. Web address is visible in address bar of all internet browsers.

d. Enable two-factor authentication for logging into email websites. If properly configured, the stolen username / passwords will be useless for hackers.

e. Ensure implementation of security measures for password recovery by entering second email or mobile number so that stolen account may be recovered.