Subject: **Prevention Against Cyber Espionage (Advisory No 04 Feb 2016)**

1. **Summary of Cyber Attack**

Attachment Phishing Page	**Subject:** Quotation
Purpose: To steal username and password of from users of sensitive organization	

2. **Indicators of Compromise.** Following are the qidicators of attack:-

a. Opening the link in email redirects the user to following Phishing page-

(1) http://damoscope.com/redux/broom/exc.php?

3. **Method of Operation.** A target receives an email with the mentioned subject which contains link to Phishing page. It asks user to enter the username and password. It then opens a fake outlook page and steals the credentials of user.

4. **Recommendation**

a. Avoid spoofed emails/subjects and mark them as spam.

b. Change password of online account immediately.

c. Enable 'Two Factor Authentication" in email accounts.

d. Verify the address of such phishing links in "status bar" of. web browser before opening it.

e. Use chrome or firefox and install plUgin "Web of Trust" to view rating of page before opening it.

f. Install well reputed antivirus/firewall software that block known malwares.

(1) Bitdefender total security.

(2) Kaspersky internet security.

(3) Eset N0D32 internet security.