Subject:- **PREVENTION AGAINST CYBER ESPIONAGE (ADVISORY NO 15, NOV 2015)**

1. Summary of cyber attack

Phishing Link: Annex A	**Subject;** Documentaries
Purpose: To steal credentials of email account from users of sensitive organizations	

2. Indicators of Compromise. Following indicates whether Phishing attack has hacked the email account or not.

a. Loss of username and password of email account.

b. Fake Google Docs Page with following address in the address bar of browser http://wwww.stcatharinesfeis.com/cgi/aos/index.htm (Annex B)

3. Method of Operation . Following is the method of infection that enables hackers to steal credentials of email**:-**

a. Asks user to click on the link to view encrypted document uploaded on Google Document**.**

4. Recommendations. In order to enhance security against attempts of stealing credentials, following is suggested:-

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

b. Install well reputed antivirus/firewall software that fan block known phishing sites such as:-

(1) Bit defender total security.

(2) Kaspersky internet security.

(3) Eset NOD32 internet security.

c. Change password of account immediately.

d. Enable "Two Factor Authentication" in email accounts.

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

f. Check the address in phishtank.com which is a anti phishing site.